AUDIT OF THE DEPARTMENT OF JUSTICE INFORMATION TECHNOLOGY STUDIES, PLANS, AND EVALUATIONS

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 07-39
August 2007

AUDIT OF THE DEPARTMENT OF JUSTICE INFORMATION TECHNOLOGY STUDIES, PLANS, AND EVALUATIONS

EXECUTIVE SUMMARY

Background

This report is the final in a series of three reports prepared by the Department of Justice (Department) Office of the Inspector General (OIG) in response to a congressional request included in the Department's appropriation for fiscal year (FY) 2006. Specifically, Congress instructed the OIG to present to the Committees on Appropriations: (1) an inventory of all major Department information technology (IT) systems and planned initiatives, and (2) a report that details all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives. Congress requested that the OIG include an analysis identifying the depth and scope of problems the Department has experienced in the formulation of its IT plans.

The OIG's first report, issued in March 2006, presented an unverified inventory of the Department's major IT investments based on information reported to the Office of Management and Budget (OMB) for budget purposes. The inventory contained 46 major investments, each with projected costs at or exceeding $15 million for FYs 2005 through 2007.

The second report, issued in June 2007, presented the refined inventory of major systems according to criteria developed by the OIG, reducing the number of major systems to 38. The second report also examined issues related to verifying cost information about the 38 systems.

This third and final report addresses the request for the OIG to prepare a report that details the research, plans, studies, and evaluations related to the Department's information technology initiatives. This report also includes an analysis of problems related to IT planning that have been identified in previous OIG reports.

Our work involved the Department's Office of the Chief Information Officer and eight of the Department's components or offices. We generally focused our audit on the 38 major systems and initiatives that were identified in the refined OIG inventory. These included the following number of systems in the chart below for each of the Department's components represented in the revised inventory.

Component	*Number of Systems*
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)	1
Bureau of Prisons (BOP)	1
Drug Enforcement Administration (DEA)	6[1]
Executive Office for Immigration Review (EOIR)	1
Federal Bureau of Investigation (FBI)	21
Justice Management Division (JMD)	6
Office of the Deputy Attorney General (ODAG)	1
Office of Justice Programs (OJP)	1
Total	38

Source: Department of Justice, Office of the Inspector General

The types of systems, stages of development, and scopes of the projects vary widely. The systems include infrastructure acquisitions and application development projects that are in the early phases of planning and others that had been operational for several years.

OIG's Audit Approach

Our audit objectives were to: (1) identify all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives; and (2) analyze the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

We identified relevant federal, Department, and component-specific requirements and standards for IT research, studies, plans, and evaluations, and merged the various standards into a generic set of documents. We requested and obtained documents from the components to develop the inventory, and assessed compliance with the document standards for the major systems in the inventory. For this audit report, we focused specifically on studies and research that justified the selection of investments in the OIG's revised inventory of major IT systems and projects, plans that were developed after the investments were authorized, and evaluations that were performed after systems were implemented.

[1] In the previously issued OIG report on Identification and Review of the Department's Major Information Technology Systems Inventory, which provides information on the cost of the Department's major IT systems, we included seven systems for the DEA and none for the ODAG. The seven systems included the Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center System (OFC) because the DEA's unobligated funds developed the OFC. However, in this report we include the OFC as part of the ODAG because the system actually resides in that office.

To evaluate problems the Department has experienced in its IT planning, we analyzed the evaluations obtained for information about problems the Department has experienced in formulating IT plans. We reviewed relevant audit and other independent reports, extending the scope of our audit work to some systems and projects that were not included in the inventory of major systems. We also asked the components to inform us of IT projects that had been terminated or had experienced problems.

IT Management

The Deputy Assistant Attorney General for Information Resources Management (DAAG/IRM), who reports to the Assistant Attorney General for Administration, serves as the Department's Chief Information Officer (CIO). The CIO's responsibilities include establishing and implementing Department-wide IT policies and standards, developing the Department's IT Strategic Plan, and reviewing and evaluating the performance of the Department's IT programs and projects. In his role as the DAAG/IRM, the CIO leads the Information Resources Management (IRM) office of the Justice Management Division (JMD).

JMD developed and operates many systems that serve more than one component in the Department. The Department's other components are responsible for providing information to the CIO, demonstrating that resources are being well spent and managed, and using the methodology in the Department's standards for information systems. Each of the components included in the revised inventory has its own CIO, except for the Office of the Deputy Attorney General.

Numerous federal, Department, and component guidelines establish criteria for IT research, studies, plans, and evaluations. The guidelines come from both IT and budget authorities, and can apply to the Department as a whole or to individual components, such as the DEA or FBI. The various standards should complement one another. However, the IT compliance environment is complex and involves strategic planning, IT development methodologies, IT investment management, enterprise architecture, procurement, and budgeting.[2] Additionally, many standards exist as guidelines rather than requirements, and allow flexibility for variation.

[2] Enterprise architecture (EA) is a blueprint that explains and guides how an organization's IT and information management elements work together to accomplish the mission of the organization. An EA addresses business activities and processes, data sets and information flows, applications and software, and technology.

IT projects can be expected to go through a process of identifying a business need and alternative solutions for meeting the need, selecting the best alternative, planning to acquire or build the solution, defining specific requirements, and designing, building, testing, implementing, and evaluating the implemented solution. The Department's Systems Development Life Cycle Guidance Document (SDLC) describes 10 life-cycle phases with associated tasks and deliverable products, including specific studies, plans, and evaluations. For different types of acquisitions and smaller-scope projects, the life-cycle work pattern can be tailored to reduce the workload from a full sequential work pattern. Tailoring the work pattern may include dropping requirements for specific tasks, studies, plans, and evaluations. Different sets of deliverables are identified in other standards, such as the Department's Information Technology Investment Management Guide (ITIM Guide) and the FBI's Life Cycle Management Directive (LCMD).[3]

Both the SDLC and ITIM tasks and deliverables generally follow the progression of IT projects chronologically. Under both, studies and research, such as alternatives analyses, feasibility studies, risk analyses, and market research for possible solutions, are performed early in the life of a system as the basis for selecting the best alternative and preparing the business case for the project. Major plans of all types, such as project management plans and quality assurance plans, are developed after the selected approach has been authorized. Post-implementation reviews, in-process review reports, and user satisfaction reviews are types of evaluations that occur after an IT system has been implemented or a project has been terminated. We used this chronological approach to identify and organize the studies, research, plans, and evaluations that are addressed in this audit.

This chronological approach is qualified by the evolutionary nature of the entire life-cycle process. As projects evolve to become more defined over time, plans should also become more defined. The life cycle of identifying business needs, selecting best alternatives, determining which IT investments should be added to and continued in the Department's portfolio, acquiring and building solutions, and evaluating the results is intended to be iterative and ongoing. Both the SDLC and ITIM also require various types of ongoing evaluations to occur regularly as decision points are reached during the course of IT projects.

[3] ITIM processes help identify needed IT projects, select new projects, and track and oversee project costs and schedules. The LCMD is the FBI's systems development life cycle guidance defining IT project management procedures and documentation requirements.

Department IT Studies, Plans, and Evaluations

Two comprehensive IT plans for the Department are required by Office of Management and Budget (OMB) standards: the Department's IT Capital Plan and IT Strategic Plan. The IT Capital Plan, *Agency IT Investment Portfolio*, described in the second of the OIG's three IT reports, represents the Department's inventory of major IT investments. For this audit, we reviewed the Department's IT Strategic Plan, which is described in Finding 1 of this report. Components are also allowed to develop their own IT strategic plans, as long as they are consistent with the Department's plan.[4] Five of the components we reviewed had developed their own IT strategic plans. The IT strategic plans are listed in Appendix III of this report. All other documents described in Finding 1, "Studies, Plans, and Evaluations," were prepared in response to standards associated with each system or initiative.

Studies required by the various standards for IT activities and documents associated with each IT system or project are generally prepared early in the life cycle of an IT project to identify and evaluate possible alternative solutions to meet a business need. The studies include market research, alternative analyses, feasibility studies, cost-benefit analyses (or benefit-cost analyses), risk analyses, and privacy impact assessments.

The plans specified by the Department's SDLC for each IT system or project include many types that are developed after an alternative solution has been selected. These include the following plans.

- risk management
- acquisition
- project management
- system security
- systems engineering management
- configuration management
- quality assurance
- validation and verification
- testing
- conversion
- implementation
- training
- contingency
- disposition

For evaluations, we requested reports of evaluations specified in the SDLC, such as post-implementation review reports, in-process review reports, and user satisfaction review reports. Post-implementation reviews are conducted after a system has been in production for a period of time and are used to evaluate the effectiveness of the system development. The

[4] DOJ Order 2880.1B, Information Resources Management Program, allows, but does not require, components to develop their own IT strategic plans.

review should determine whether the system does what it was designed to do, supports users as required, and was successful in terms of functionality, performance, and cost benefit. It should also assess the effectiveness of the development activities that produced the systems. The review results should be used to strengthen the systems as well as system development procedures. In-process reviews are performed during operations and maintenance to assess system performance and user satisfaction, and should occur repeatedly after a system has been implemented to ensure the system continues to meet needs and perform effectively.

Components submitted more than 800 items that we accepted as responsive to our requests. Of the 800 items, 494 were entire documents we categorized as studies, plans, and evaluations, which we included in our list of documents. The other items submitted by components were artifacts or other products of the system development and acquisition process. Artifacts included items such as briefing slides, spreadsheets showing schedules and work breakdown structures, and various progress reports. The studies, plans, and evaluations are listed in Appendix V to this report.

While many of the documents specified in various guidelines were produced, significant gaps existed between the studies, plans, and evaluations described in the guidelines and what was prepared by the components. Only seven post-implementation evaluations were obtained, of which four did not reflect lessons learned in terms of project planning and management.

We found the highest levels of compliance in the areas of business case documents, which become part of the Department's annual budget process and are required to obtain funding for each system or project, and security plans, which are required for projects to obtain authorization to operate. The components provided at least one business case document for 36 of the 38 systems in the inventory. The two exceptions, the FBI's Investigative Data Warehouse (IDW) and Secure Compartmented Information Operational Network (SCION), are included in an "umbrella" business case that represents the Department's consolidated enterprise infrastructure (CEI). The business case document represents the single document type for which we found 100 percent compliance.

System security plans also had a high level of compliance. We obtained system security plans for 32 of the 38 projects. The six other projects were either too early in the life cycle for preparation of this document, or a draft security plan was undergoing review. Components also demonstrated a high level of compliance with privacy impact assessments (PIA), and we found acceptable explanations for the projects that did not

submit a PIA. Components provided project management plans for 29 of the 38 projects, and explained all but one of those exceptions.

However, we found compliance in the areas of systems engineering management, configuration management, quality assurance, validation and verification, and training plans was significantly lower. The components cited several different reasons for not providing documents relating to these issues that we requested. The reasons included: (1) the requirement was not applicable to the investment; (2) a waiver to the requirement had been granted; (3) planning for the system pre-dated FY 2000 and the documentation was not available; (4) the system was purchased commercially off-the-shelf eliminating the need for certain processes; and (5) the investment had not reached the applicable point in the life cycle.

Department oversight is designed to focus on the capital planning and investment control (CPIC) process concerned with selecting and prioritizing IT investments. According to JMD officials and DOJ Order 2880.1b, Department oversight is not designed to enforce policies and procedures on documentation.[5] JMD officials told us they do not perform independent reviews of the other components' IT projects, nor do they receive major studies, plans, and evaluations from the components to review. The Department-level oversight of major IT projects is performed through presentations to the Department's Investment Review Board, the CIO's Dashboard report, and through the OMB exhibit 300s, all of which are described in the second report in this series. This allows some tracking of actual performance against scheduled milestones and costs, but does not involve JMD officials in the details of IT documentation for individual projects.

Based on the limited number of certain types of plans and evaluations produced on these major systems and projects, we recommend that the CIO evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects.

Many standards exist that define the types of studies, plans, and evaluations that should be performed for individual projects. The standards allow significant flexibility through waivers of document requirements and tailoring of the processes. For example, the SDLCs and FBI's LCMD encourage tailoring the documentation standards to the size and complexity of the project. Although the SDLCs specify many studies, plans, and

[5] The CIO does have specific responsibilities to enforce security standards.

evaluations for all types of projects in the tailoring guidelines, we found that many Department projects have not generated these "required" documents. It is possible that the standards are not necessarily appropriate to different types of projects or acquisitions and should be revised. The Department should exercise increased oversight of the tailoring being done, and consider revising the guidelines for tailoring the work pattern for specific types of projects.

IT Planning Problems

To identify problems the Department has experienced in planning for IT systems and projects, we reviewed previous OIG audits and other reports. We also reviewed the evaluations we obtained from the components to help identify problems the Department has experienced in planning for IT systems.

We asked components for information on IT projects that had failed or been terminated. Other than one portion of the FBI's Trilogy project and the FBI's Laboratory Information Management System (LIMS) project, the components told us they were not aware of failed or terminated projects. The OIG found during work on the second report in this series that JMD's Justice Consolidated Office Network (JCON) project had experienced a project termination sometime before FY 2002 prior to the current project. JMD, however, was not able to provide any information about the failure. The fact that no evaluation was performed to assess reasons for the failure suggests a serious gap in standards for evaluations. Terminated projects should be evaluated to determine the causes of the problems.

We also found that the Department had produced few evaluations of project management or success for IT projects in post-implementation reviews. According to the DOJ SDLC, one purpose of post-implementation reviews is to assess the effectiveness of the life-cycle development activities that produced the system. This includes analyzing if proper limits were established in the feasibility study and if the limits were maintained during implementation, addressing the reasons for variances between planned and realized benefits, addressing the reasons for differences between estimated and actual costs, and evaluating whether training was adequate, appropriate, and timely. The review results are intended to be used to strengthen the system development procedures, as well as the system itself.

The DOJ ITIM Guide calls for continuous monitoring of investments to assess progress against established cost, schedule, and performance metrics in order to mitigate any risks or costs on an on-going basis. The DOJ ITIM Guide also indicates that the activities of the evaluation phase include

applying lessons learned from post-implementation reviews and periodic operational analyses for ITIM process improvement. The lessons learned for ITIM process should be incorporated into the select and control phases for future IT investments.

The OIG has issued audit and inspection reports about IT systems and project management that have focused on various IT concerns. These include the management and progress of individual IT projects, IT management in general, the performance of individual systems following implementation, system security, and system controls in financial management systems. Appendix VII lists prior OIG audits and inspections on IT issues that we reviewed for this analysis.

Among the problems that have been described in previous audit reports related to IT planning were weaknesses in investment and program management practices, business process re-engineering (BPR), cooperation between agencies, and contract management. BPR is defined as the redesign of the organization, culture, and business processes using technology as an enabler to achieve significant improvements in cost, time, service, and quality.

For example, various contracting and program management weaknesses contributed to the failure of the FBI's Virtual Case File (VCF) project. The FBI did not effectively oversee the contract and failed to establish firm milestones to be achieved before the project could move to the next phase. In the FBI's LIMS project, the OIG found that firmly managed schedule, cost, technical, and performance benchmarks for the contract would have raised warning signs earlier in the project and perhaps led to resolution of the problems encountered.[6]

The DOJ System Development Life Cycle Guidance Document indicates that business process re-engineering (BPR) should be the underpinning of any new system development or initiative, as part of strategic planning for information systems, and that agencies should consider BPR before requesting funding for a new project or system development effort. However, reviews have raised issues related to weaknesses in business process re-engineering in the planning of the Department's IT projects. One study of the FBI's terminated VCF project found that senior managers were not involved in efforts to re-engineer business processes or in rethinking the FBI's use of IT, and that while users working on the re-engineering were

[6] The FBI's Laboratory Information Management System (LIMS) project contract was terminated after the FBI determined the system would not be able to meet security requirements. See the discussion in Finding 2.

experienced agents, none had experience with complex IT development projects or business process re-engineering.

Requirements planning is another area that has been cited as weak in specific audit reports. For example, the LIMS project was terminated in large part due to problems with the security requirements of the system, which were not fully defined early in the project. The LIMS Request for Proposal (RFP) had required security to be part of the system, but the FBI strengthened its security requirements after the contract award following high-profile espionage-related security breaches in the FBI. The audit found that the FBI had failed to document security requirements adequately and, to the extent the security requirements evolved, did not clarify those changes through contract modifications.

Conclusion

This audit sought to identify research, plans, studies, and evaluations that the Department has produced or is in the process of producing concerning IT systems, needs, plans, and initiatives. In addition, we analyzed the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

Components submitted 494 documents that we categorized as studies, plans, and evaluations, related to federal, Department, and component-specific requirements and standards. Many of the documents specified in various criteria were produced, but significant gaps existed between the studies, plans, and evaluations described in criteria and what was prepared.

We found the highest levels of compliance in the areas of business case documents, which become part of the Department's annual budget process and are required to obtain funding for each system or project, and security plans, which are required for projects to obtain authorization to operate. The components provided at least one business case document for 36 of the 38 systems in the inventory. The two exceptions, the FBI's Investigative Data Warehouse (IDW) and Secure Compartmented Information Operational Network (SCION), are included in an "umbrella" business case that represents the Department's consolidated enterprise infrastructure (CEI).

System security plans also had a high level of compliance. We obtained security plans for 32 of the 38 projects. The six other projects were either too early in the life cycle for preparation of this document, or a draft security plan was undergoing review. Components also demonstrated a high level of compliance with privacy impact assessments (PIA), and we

found acceptable explanations for the projects that did not submit a PIA. Components also provided project management plans for 29 of the 38 projects, and explained all but one of those exceptions.

However, we found compliance in the areas of systems engineering management, configuration management, quality assurance, validation and verification, and training plans was significantly lower. In addition, components provided only seven post-implementation review reports.

Prior OIG reports have identified planning problems on individual systems and projects that include weaknesses in business process re-engineering, requirements planning, cooperation between agencies, and IT program and contract management. These weaknesses have contributed to:

- project re-starts, cost increases, and delays in the FBI's implementation of a case management system,
- the termination of the FBI's LIMS project,
- delays in implementing an interoperable fingerprint identification system that can be used by both the Department and federal immigration authorities, and
- data integrity problems in the TSC database.

We originally planned to use evaluations we obtained from components to identify problems the Department has experienced in planning for IT systems. This was not possible because the Department has produced so few evaluations of project management for either successful or failed IT projects, with the exception of two terminated projects in the FBI.

In this report, we made five recommendations to the Department, such as recommending that the Department evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects. We also recommend that the Department consider revising the guidelines for tailoring the work pattern for specific types of projects. Additional recommendations focus on improving the evaluation of IT project management in the Department and improving business process re-engineering, and contract management and oversight. We believe the Department should ensure that evaluations are performed on both implemented systems and terminated projects that focus on lessons learned on planning and project management issues.

Table of Contents

INTRODUCTION

Background

This report is the final in a series of three reports prepared by the Department of Justice (Department) Office of the Inspector General (OIG) in response to a congressional request included in the Department's appropriation for fiscal year (FY) 2006. Specifically, Congress instructed the OIG to present to the Committees on Appropriations: (1) an inventory of all major Department information technology (IT) systems and planned initiatives, and (2) a report that details all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives. Congress requested that the OIG include an analysis identifying the depth and scope of problems the Department has experienced in the formulation of its IT plans.

The OIG's first report, issued in March 2006, presented an unverified inventory of the Department's major IT investments based on information reported to the Office of Management and Budget (OMB) for budget purposes.[7] The inventory contained 46 major investments, each with projected costs at or exceeding $15 million for FYs 2005 through 2007.

The second report, issued in June 2007, presented the refined inventory of major systems according to criteria developed by the OIG, reducing the number of major systems to 38.[8] The second report also examined issues related to verifying cost information about the 38 systems.

This third and final report addresses the request for the OIG to prepare a report that details the research, plans, studies, and evaluations related to the Department's information technology initiatives. We used the refined inventory of major systems presented in the second report to focus our work for this current report. This report also includes an analysis of problems related to IT planning that have been identified in previous OIG reports.

---

[7] Department of Justice, Office of the Inspector General, *Inventory of Major Department of Justice Information System Investments as of Fiscal Year 2006,* Audit Report No. 06-25, March 2006.

[8] Department of Justice, Office of the Inspector General, *Identification and Review of the Department's Major Information Technology Systems Inventory,* Audit Report No. 07-37, June 2007.

Major Systems

We generally focused our audit on the 38 major systems and initiatives that were identified in the refined OIG inventory, which are shown in Figure 1, listed by the component within the Department that is responsible for each system.[9] The components are the:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Bureau of Prisons (BOP)
- Drug Enforcement Administration (DEA)
- Executive Office for Immigration Review (EOIR)
- Federal Bureau of Investigation (FBI)
- Justice Management Division (JMD)
- Office of the Deputy Attorney General (ODAG)
- Office of Justice Programs (OJP)

[9] For our analysis of problems the Department has experienced with planning for IT systems, we included a few additional systems and projects for which we had information about project termination or other problems. These are introduced in Finding 2.

Major Systems and Projects

Figure 1

Component	*System or Project*	*Full Title*
ATF	NIBIN	National Integrated Ballistics Information Network
BOP	ITS II	Inmate Telephone System II
DEA	Concorde	Concorde
DEA	E-Com	Electronic Commerce
DEA	EIS	El Paso Intelligence Center (EPIC)Information Systems
DEA	Firebird	Firebird
DEA	M204	Model 204 Corporate Systems
DEA	Merlin	Merlin
EOIR	eWorld	eWorld
FBI	BRIDG	Biometric Reciprocal Identification Gateway
FBI	CARTSAN	Computer Analysis Response Team Storage Area Network
FBI	CODIS	Combined DNA Index System
FBI	DCS	Digital Collection System
FBI	DCU	Data Centers Unit
FBI	EDMS	Electronic Surveillance (ELSUR) Data Management System
FBI	FTTTF	Foreign Terrorist Tracking Task Force
FBI	IAFIS	Integrated Automated Fingerprint Identification System
FBI	IATI	Information Assurance Technology Infusion
FBI	IDW	Investigative Data Warehouse
FBI	LEO	Law Enforcement Online
FBI	NCIC	National Crime Information Center
FBI	N-DEx	Law Enforcement National Data Exchange
FBI	NGI	Next Generation Identification
FBI	NICS	National Instant Criminal Background Check System
FBI	R-DEx	Regional Data Exchange
FBI	SCION	Secure Compartmented Information Operational Network
FBI	SENTINEL	Sentinel
FBI	SMIS	Security Management Information System
FBI	TRP	Technical Refreshment Program
FBI	TSC	Terrorist Screening Center
JMD	CITP	Classified Information Technology Program
JMD	IWN	Integrated Wireless Network
JMD	JCON	Justice Consolidated Office Network
JMD	LCMS	Litigation Case Management System
JMD	PKI	Public Key Infrastructure
JMD	UFMS	Unified Financial Management System
ODAG	OFC[10]	Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center System
OJP	JGMS	Justice Grants Management System

Source: Office of the Inspector General

[10] In the previously issued OIG report on Identification and Review of the Department's Major Information Technology Systems Inventory, which provides information on the cost of the Department's major IT systems, we included the OFC as part of the DEA because the DEA's unobligated funds developed the OFC. However, in this report we include the OFC as part of the ODAG because the system actually resides in that office.

These systems represent a wide range of types of systems and initiatives, including efforts to acquire infrastructure, implement communications networks, and build application programs to support business transactions. For example, the DEA's Firebird project is providing infrastructure network equipment which allows DEA staff to use various automated programs. Its Concorde project is intended to update and transition older applications that currently run on older hardware and database platforms to newer platforms. OJP's Litigation Case Management System project is a major new development effort designed to build an enterprise case management system that will serve as an infrastructure for the sharing of case-related information within and between the Department's components and United States Attorneys Offices.

The systems we reviewed are also in various stages of development and operation. Some of the systems have been in steady-state operational status for many years. Others are new development or in a mixed life-cycle phase, meaning the system is operational with significant modifications or enhancements being implemented. These variations affect which studies, plans, and evaluations have been or should have been prepared.

The OMB budget process grants agencies significant flexibility in defining what needs to be reported as an "IT investment" for budget purposes. Most of the system titles in Figure 1 represent single information systems, but others, such as the DEA's EIS and the FBI's FTTTF represent programs that include multiple information systems. JMD's Public Key Infrastructure (PKI) project is an initiative that will affect access to many other systems in the Department by specifying access controls. A brief summary on each system or project is found in Appendix VI, along with a list of the studies, plans, and evaluations we obtained associated with the project.

Information Technology Organizations

Our work involved the Department's Office of the Chief Information Officer and the eight Department components or offices listed on page 2.

Office of the Chief Information Officer (OCIO)

The Deputy Assistant Attorney General for Information Resources Management (DAAG/IRM), who reports to the Assistant Attorney General for Administration, serves as the Department's Chief Information Officer (CIO). The CIO's responsibilities include establishing and implementing Department-wide IT policies and standards, developing the Department's IT Strategic Plan, and reviewing and evaluating the performance of Department IT programs and projects. In his role as the DAAG/IRM, the CIO leads the Information Resources Management (IRM) function of the Justice Management Division (JMD).

Justice Management Division

JMD provides administrative services to the Department, including those related to human resources, controller activities, and IT systems and support. In the area of IT, JMD serves a central role for the Department for policy, planning, monitoring, and services. DOJ Order 2880.1B, Information Resources Management Program, September 27, 2005, requires the CIO, in his role as the DAAG/IRM, to deliver IT services to the Department through the JMD.[11]

JMD developed and operates many systems that serve more than one component in the Department, and it owns six of the major systems in our inventory. JMD is responsible for overseeing the development and implementation of the Unified Financial Management System, which is intended to consolidate financial reporting for all of the Department's components and replace six different financial management systems. The Litigation Case Management System will serve seven litigating divisions of the Department and will implement a common case management architecture for future projects. The Integrated Wireless Network project is intended to provide a consolidated, nationwide federal wireless communications service that will replace standalone systems in various components. The Justice Consolidated Office Network seeks to provide a reliable common office automation platform upon which 16 of the Department's litigating, management, and law enforcement components operate mission-critical applications. Under the Classified Information Technology Program, the Department will develop a classified Enterprise Architecture, an initial operational infrastructure, and an operations and

[11] A DOJ Order is a type of directive used to issue Departmental policy and direction for administrative matters.

maintenance model for processing classified information.[12] The Department has also established a Public Key Infrastructure project to enhance access security for existing applications and services. The enhanced security will support communications between Department staff and federal, state, and local government agencies.

Within the OCIO, the CIO-DAAG/IRM leads five staffs: (1) Policy and Planning, (2) Electronic Government Services, (3) Information Technology Security, (4) Operations Services, and (5) Enterprise Solutions. Of the six systems and projects in the refined inventory for which JMD is responsible, five are the responsibility of the OCIO. The following four projects are assigned to the Enterprise Solutions Staff:

- Classified Information Technology Program,
- Justice Consolidated Network,
- Litigation Case Management System, and
- Public Key Infrastructure Project.

The Integrated Wireless Network project is assigned to the Electronic Government Services Staff. The Office of the Controller, which is not a part of the IRM office, is responsible for the sixth JMD project, the Unified Financial Management System.

Component IT Organizations

Components in the Department are responsible for:

- providing information on their investments as requested by the Department's CIO;
- demonstrating that resources are being well-spent and managed;
- demonstrating that risks are being properly addressed;

[12] Enterprise Architecture (EA) is a blueprint that explains and guides how an organization's IT and information management elements work together to accomplish the mission of the organization. An EA addresses business activities and processes, data sets and information flows, applications and software, and technology.

- developing an acquisition strategy for all major IT projects;
- implementing security policies and guidelines, and
- using the methodology in the Department's Systems Development Life Cycle Guidance Document for all information systems and applications, tailored to individual projects.

Each of the components responsible for one of the major IT systems in the OIG's refined inventory has its own CIO and IT organization, with the exception of the ODAG. Many of the initiatives in the refined inventory were managed out of the CIO's offices identified in Figure 2, although some were managed by other offices within the component.

Chief Information Officers and Organizations

Figure 2

Component	*# Systems in Inventory*	*Organization*	*CIO Reports to*
JMD	6	Information Resources Management	Assistant Attorney General for Administration
ATF	1	Office of Science and Technology	Deputy Director
BOP	1	Office of the Chief Information Officer	Assistant Director for Information, Policy, & Public Affairs Division
DEA	6	Office of Information Systems	Deputy Administrator
EOIR	1	Office of Planning, Analysis & Technology	Assistant Director
FBI	21	Office of the Chief Information Officer	Associate Deputy Director
OJP	1	Office of the Chief Information Officer	Deputy Assistant Attorney General

Source: Department of Justice components. (There is also one system in the ODAG, which does not have a CIO.)

Standards for IT Studies, Plans, and Evaluations

Numerous federal, Department, and component-level guidelines establish criteria for IT research, studies, plans, and evaluations. The guidelines come from both IT and budget authorities, and may apply to the Department as a whole or to individual components such as the DEA or FBI. While the various standards should complement one another, the compliance environment is complex and involves strategic planning, IT development methodologies, IT investment management, enterprise architecture, procurement, and budgeting. Additionally, many standards exist as guidelines rather than requirements, thereby allowing needed flexibility

depending on the specific characteristics (type, size, scope, status) of each project.

Federal IT Standards

The Information Technology Management Reform Act (ITMRA) of 1996, also known as the Clinger-Cohen Act, P.L. 104-106, February 1996, requires federal agencies to improve the acquisition, use, and disposal of information technology by implementing a capital planning and investment control (CPIC) process that links to budget formulation and execution.[13] The process is intended to maximize the value, and assess and manage the risks, of IT acquisitions. This Act also requires agencies to focus information resource planning to support their strategic missions and to rethink and restructure the way they do their work before investing in information systems.

OMB Circular A-130, Management of Federal Information Resources, revised November 2000, establishes policy for the management of federal information resources, based on several laws, including the Clinger Cohen Act. The Circular assigns responsibilities to various agencies and establishes standards for the CPIC process. The CPIC process is intended to include all stages of capital programming, including planning, budgeting, procurement, management, and assessment. It requires information resource management Strategic Plans, which are strategic in nature, and IT Capital Plans, which are operational in nature. The IT Capital Plans are submitted to OMB with agency budget submissions annually, and are required to include the IT Capital Asset Plans for major information systems or projects.

The OMB also publishes guidelines governing budget submissions each year that influence IT planning and documentation. OMB Circular A-11, Preparation, Submission, and Execution of the Budget, June 2006, establishes detailed standards for the IT Capital Plans to be submitted for each budget year. Two main exhibits are submitted with the Department's budget each year representing the Department's IT Capital Plan. Under the Circular's Part 2, Preparation and Submission of Budget Estimates, Section 53, Information Technology and e-Government, federal agencies are required to submit an Agency IT Investment Portfolio, called the OMB

[13] The Clinger-Cohen Act is Division E of the National Defense Authorization Act for Fiscal Year 1996.

exhibit 53, which is a table of basic information about each major IT investment. Section 53 also requires the submission of Privacy Impact Assessments (PIA), one of the studies we have included in our audit.

Circular A-11's Part 7, Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets, requires agencies to provide an IT Capital Asset Plan and Business Case (exhibit 300) for each major IT investment that is included in the portfolio. This part also generally establishes policy for planning, budgeting, acquiring, and managing federal capital assets, and provides instructions on budget justification and reporting requirements for major information technology investments. Each exhibit 300 is required to contain information demonstrating compliance with OMB's CPIC policies and with OMB Circular A-130 and E-Gov related policy memoranda. Agencies justify new or continued funding for major acquisitions by demonstrating on exhibits 300:

- a direct connection to the agency's strategic plan,
- a positive return on investment for the selected alternative,
- sound acquisition (program and procurement) planning,
- comprehensive risk mitigation and management planning,
- realistic cost and schedule goals, and
- measurable performance benefits.

In addition, agencies are expected to document detailed information substantiating the portfolio of major investments in accordance with the agency's capital programming process.

The OMB's *Capital Programming Guide*, *Supplement to OMB Circular A-11, Part 7*, *Planning, Budgeting, and Acquisition of Capital Assets,* June 2006, contains more detailed guidance to federal agencies about practices and lessons learned for more efficient project and acquisition management of capital assets. It integrates various statutory and management initiatives into a single, integrated capital programming process to ensure that capital assets successfully contribute to the achievement of agency strategic goals and objectives. Its purpose is to assist federal agencies in planning, procuring, and using capital assets to achieve the maximum return on investment.

Additionally, numerous laws and standards exist regarding specific financial systems, system security, enterprise architectures, electronic access, and data quality. Because these standards focus on specific system requirements rather than on IT planning and evaluation processes, we did not use these as the basis for determining IT planning and evaluation requirements, and they are not included in this report.

Department Standards

The Department has implemented a number of standards that define IT processes and result in studies, plans, and evaluations. DOJ Order 2880.1B, Information Resources Management Program, September 2005, establishes the CIO's authority for issuing Department-wide IT policies, standards, and guidelines, and for reviewing and evaluating the performance of IT programs and projects.

The Department's Guide to the DOJ Information Technology Investment Management (ITIM) Process (ITIM Guide), August 2001, implemented the capital planning and investment control process that was required by the Clinger-Cohen Act.[14] The ITIM Guide integrates the interrelated disciplines of strategic planning, performance planning, systems life-cycle development, capital planning, security, architecture, and acquisition planning, and program management. Intended to complement the Systems Development Life Cycle process already in place, it defines criteria for "major" information systems in the Department and specifies a number of documents that should be produced as part of each phase of IT management.

The Department's Systems Development Life Cycle (SDLC) Guidance Document, revised January 2003, establishes life-cycle management procedures, practices, and guidelines governing IT work within the Department. The guidance is intended to be used for all of the Department's information systems and applications, but is also intended to allow flexibility to suit the characteristics of particular development efforts. Tailoring standards may be based on individual project cost, complexity, and criticality to the agency's mission. When a full sequential life-cycle pattern is not appropriate, the SDLC offers alternate work patterns for smaller or more limited efforts, such as implementing commercial-off-the-shelf (COTS) products.

[14] ITIM processes help identify needed IT projects, select new projects, and track and oversee project costs and schedules.

Component-Specific Standards

Each of the Department's components may establish its own life-cycle guidelines as long as they are consistent with the Department's standards. For this audit, we found that the BOP, EOIR, and JMD use the Department's SDLC. The DEA and FBI developed their own life-cycle development methodologies defining IT project management procedures and documentation requirements – the DEA System Development Life Cycle (DEA SDLC), March 2000, and the FBI Life Cycle Management Directive (FBI LCMD), August 2005, which was first implemented in November 2004.[15]

The DEA SDLC closely follows the Department's life-cycle guidance in terms of the phases of development and documents described. The FBI LCMD is a more recent methodology and more closely resembles elements of the CPIC process. Some of the documents required by the FBI LCMD are virtually identical to aspects of the Capital Asset Plan and Business Case (exhibit 300) that is to be submitted to the OMB for each major IT investment. Details about the requirements under each methodology for the studies, plans, and evaluations included in this audit are found in the detailed discussion of each document type in Finding 1. All of the Department's components included in this audit allow some variation within their own IT development standards.

IT System Life-Cycle Concepts

Projects can be expected to go through a process of identifying a business need and alternative solutions for meeting the need, selecting the best alternative, planning to acquire or build the solution, defining specific requirements, and designing, building, testing, implementing, and evaluating the implemented solution. The Department's SDLC Guidance Document describes 10 phases of IT work: initiation, concept development, planning, requirements analysis, design, development, integration and test, implementation, operations and maintenance, and disposition of information systems within the Department. The SDLC specifies tasks and deliverables, including planning documents, to be created for each of the phases.

For different types of acquisitions and smaller-scope projects, the life-cycle work pattern can be tailored to reduce the workload from a full sequential work pattern. Tailoring the work pattern may include dropping

[15] The U.S. Marshals Service (USMS) also developed its own SDLC, but there were no USMS systems in the revised inventory used as the basis for this audit.

requirements for specific tasks, studies, plans, and evaluations. The major tasks and deliverables for each SDLC phase are summarized in Figure 3.

Systems Life Cycle Phases & Documents

Figure 3

Phase	***Phase Description***	***Deliverables***
Initiation	When a business need or opportunity is identified, • the business need is documented in the Concept Proposal.	Concept Proposal
System Concept Development	Once the Concept Proposal is accepted: • approaches for accomplishing the concept are reviewed for feasibility and appropriateness, and • the scope of the system is documented in the System Boundary Document.	System Boundary Document Cost Benefit Analysis Feasibility Study Risk Management Plan
Planning	When senior officials have approved the Boundary Document and some funding: • the concept is further developed to describe how the business will operate once implemented, and to assess impacts. • budget, resources, activities, schedules, tools, and reviews are defined. • system security requirements are identified and a high level vulnerability assessment is completed.	Acquisition Plan Configuration Management Plan Quality Assurance Plan Concept of Operations System Security Plan Project Management Plan Validation & Verification Plan Systems Engineering Management Plan
Requirements Analysis	• All requirements (functional, data, system performance, security, maintainability) are formally defined to a level of detail sufficient for systems design to proceed.	Functional Requirements Document Test and Evaluation Master Plan Interface Control Document Privacy Impact Assessment
Design	• Physical characteristics of the system are specified. • Detailed logical specifications are prepared. • Operating system environment is defined. • Major subsystems, inputs & outputs are defined. • Subsystems are partitioned into design units or modules.	Security Risk Assessment Conversion Plan System Design Document Implementation Plan Maintenance Manual Ops/System Administration Manual Training Plan User Manual
Development	• Detailed specifications are translated into hardware, communications, and software programs. • Software is unit tested, integrated, and retested. • Hardware is assembled and tested.	Contingency Plan Software Development Document System Application Software Test Files/Data Integration Document
Integration & Test	• All components of the system (hardware, software, interfaces, operators, users, etc.) are integrated and tested.	Test Analysis Report Test Analysis Approval Determination Test Problem Report Security Certification & Accreditation
Implementation	• The system is installed and made operational in a production environment.	Delivered System Change Implementation Notice Version Description Document Post-Implementation Review

Phase	*Phase Description*	*Deliverables*
Operations & Maintenance	The operation is ongoing and continues as long as the system can be adapted effectively to respond to needs. • The system is monitored for continued performance with requirements. • Modifications are incorporated; the system may re-enter planning phase when modifications are identified as necessary.	In-Process Review Report User Satisfaction Review Report
Disposition	Phase ensures the orderly termination of the system and preserves system data and information about the system. • Data are migrated effectively to another system or archived for future access.	Disposition Plan Post-Termination Review Report Archived System

Source: Department of Justice Systems Development Life Cycle Guidance Document, January 2003

The Department's ITIM process describes three phases: Select, Control, and Evaluate. The DOJ ITIM Guide also defines major tasks and deliverables associated with each of the three phases. The tasks and deliverables focus on the investment management process in the Department, rather than on the details of each system or project. There is some overlap between the SDLC and ITIM tasks and deliverables, but they do not precisely coincide because the focus of each is different. The ITIM phases and deliverables are summarized in Figure 4.

DOJ ITIM Process

Figure 4

Phase	*Phase Description*	*Selected Deliverables*
Select	Concept Development Business Case Analysis & Investment Proposal Development Portfolio Prioritization/Budgeting	Concept Proposal Business Case Analysis Initial Project Plan IT investment portfolio Annual briefing to CIO Budget submission
Control	Project Planning Acquisition and Development Deployment	Project Management Plan Acquisition Plan Baseline milestones and measures Earned value management system (EVMS) & work breakdown structures (WBS) with corresponding reporting mechanisms Executed contract Progress reports Periodic executive reviews/portfolio assessments Updated project documentation Periodic reviews to executives Operational system successfully deployed

Phase	*Phase Description*	*Selected Deliverables*
Evaluate	Management-In-Use	Post Implementation Review Reports Periodic Operational Analysis Reports User Survey Results
	Retirement Planning & Disposal	Asset Disposal and Data Conversion Plan

Source: DOJ ITIM Guide

Both the SDLC and ITIM tasks and deliverables generally follow the progression of IT projects chronologically. Under both, studies and research, such as alternatives analyses, feasibility studies, risk analyses, and market research for possible solutions are performed early in the life of a system as the basis for selecting the best alternative and preparing the business case for the project. Major plans of all types, such as project management plans and quality assurance plans, are developed after the selected approach has been authorized. Post-implementation reviews, in-process review reports, and user satisfaction reviews are types of evaluations that occur after an IT system has been implemented or a project has been terminated. We used this chronological approach to identify and organize the studies, research, plans, and evaluations that are addressed in this audit.

This chronological approach is qualified by the evolutionary nature of the entire life-cycle process. As projects evolve to become more defined over time, plans should also become more defined. The life cycle of identifying business needs, selecting best alternatives, determining which IT investments should be added to and continued in the Department's portfolio, acquiring and building solutions, and evaluating the results is intended to be iterative and ongoing. Both the SDLC and ITIM require multiple iterations of various documents, with updates as projects become more defined and change over time. Both the SDLC and ITIM also require various types of ongoing evaluations to occur regularly as decision points are reached during the course of IT projects.

Audit Approach

Our audit objectives were to: (1) identify all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives; and (2) analyze the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

We identified relevant federal, Department, and component-specific requirements and standards for IT research, studies, plans, and evaluations, and merged the various standards into a generic set of requirements and

standards. We requested and obtained documents from the components related to 38 major Department IT projects listed in our inventory, and assessed compliance with the document standards for the major systems in the inventory.

For this audit report, we focused specifically on studies and research that justified the selection of investments in the revised inventory of major IT systems and projects, plans that were developed after the investments were authorized, and evaluations that were performed after systems were implemented. We did not request every document specified by the DOJ SDLC or ITIM Guide, such as early plans that were developed before projects received authorization (system boundary documents) and specification and design documents.[16]

To evaluate problems the Department has experienced in planning, we reviewed relevant audit and inspection reports, extending the scope of our audit work to several systems and projects that were not included in the inventory of major systems. We analyzed these evaluations for information about problems the Department has experienced in formulating IT plans.

[16] Although a case can be made that all these documents are planning documents, it was not feasible in the course of one audit to assess entire documentation libraries for multiple projects.

FINDINGS AND RECOMMENDATIONS

Finding 1: Studies, Plans, and Evaluations

With respect to the 38 major IT systems examined in this phase of the review, components submitted 494 documents we categorized as "studies, plans, and evaluations." Some systems had up to 30 associated planning documents, while others had as few as 2. While many of the documents specified in various federal, Department, and component-level IT development standards were produced, significant gaps existed between the suggested studies, plans, and evaluations and what components prepared for individual projects. For example, components developed few post-implementation evaluations of how the systems performed and what lessons were learned during development of the system. Moreover, the OIG found that the standards for preparing studies, plans, and evaluations as part of the IT development process come from a variety of different sources that overlap, duplicate effort, and may prove cumbersome.

Inventory of Studies, Plans, and Evaluations

To identify specific IT research, studies, plans, and evaluations, we interviewed Department officials and reviewed the guidelines described in the Introduction to this report. We used the guidelines listed in Figure 5 as the basis for requesting specific studies, plans, and evaluations of IT needs, opportunities, projects, and systems. Each of the guidelines in Figure 5 is described in the Introduction to this report.

Guidelines for IT Studies, Plans, and Evaluations

Figure 5

Guideline and Date	*Applies to*
DOJ Systems Development Life Cycle Guidance Document, revised 2003	Department of Justice
Guide to the DOJ Information Technology Investment Management (ITIM) Process, August 2001	Department of Justice
DOJ Order 2880.1b, Information Resources Management Program, September 2005	Department of Justice
OMB Circular A-11, Preparation and Submission of Budget Estimates, June 2005	All Federal agencies
DEA Systems Development Life Cycle Guidance Document, March 2000	Drug Enforcement Administration
FBI Life Cycle Management Directive, revised August 2005	Federal Bureau of Investigation

Sources: Department of Justice components

We used the DOJ SDLC as the primary criterion to identify the studies, plans, and evaluations that should be prepared when developing and implementing IT projects. The standards use various names for documents and organize the information differently. For this report, we combined the various specific standards into a generic set of studies, plans, and evaluations that could be applied to all of the IT systems and projects in our inventory. Because we found little research documented outside of the OMB exhibit 300, we included "research documents" under the category of "studies."

We requested specific documents directly from each of the components because the CIO's office did not maintain major documents produced for component-specific systems. OCIO officials told us that Department oversight is designed to focus on the Capital Planning and Investment Control process for selecting and prioritizing IT investments. It is not designed to enforce policies and procedures on IT project documentation.[17] Department-level oversight of individual IT projects is performed through presentations to the Departmental Investment Review

[17] The CIO does have specific responsibilities to enforce security standards.

Board, the CIO's Dashboard report, and through the OMB exhibit 300s, all of which are described in the second report in this series. This oversight includes tracking of actual performance against scheduled milestones and costs, but does not involve JMD officials in the details of IT documentation for individual projects.

In addition to requesting specific documents, we also asked the components to provide any additional documents they had prepared that would qualify as IT studies, research, plans, or evaluations. We requested a slightly different list of documents from the FBI than from the other components because some of the FBI's LCMD standards varied somewhat from the standards being used by the other components. The variations for different components are described later in the report in the discussion of each document type. We found that the standards for preparing studies, plans, and evaluations as part of the IT development process come from a variety of different sources that overlap, duplicate effort, and may prove cumbersome.

We combined the various specific requirements from each guideline into the following generic set of criteria for studies, plans, and evaluations that we could apply to all of the IT systems and projects in our inventory. Figure 6 lists the generic set of documents we requested. All of the documents listed below are applicable to each IT system or project with the exception of an IT strategic plan, which is required for the Department but optional for components.

Studies, Plans, and Evaluations Requested

Figure 6

- Business case studies
- Market research
- Alternatives analyses
- Feasibility studies
- Cost benefit analyses
- Privacy impact assessments
- IT strategic plans
- Risk management plans
- Acquisition plans
- Project management plans
- System security plans
- Systems engineering management plans
- Configuration management plans
- Quality assurance plans
- Validation and verification plans
- Test plans
- Conversion plans
- Implementation plans
- Training plans
- Contingency & continuity of operations plans
- Disposition plans
- Test reports
- Ongoing reviews of project status and earned value management
- Post-implementation review reports
- Any other IT-related research, plans, studies, and evaluations the component performed or sponsored

Source: OIG compilation of standards

Department components submitted more than 800 documents and other evidence that we accepted as responsive in some way to our requests. Of these responses, 494 were complete documents representing studies, plans, and evaluations. The responses also included other products or artifacts of the system acquisition and development process. Artifacts included items such as briefing slides, spreadsheets showing schedules and work breakdown structures, portions of the OMB exhibit 300, and various forms of progress reports. We included other artifacts in this report to the degree that they contributed to compliance with the various standards for documentation.

A detailed listing of the studies, plans, and evaluations we obtained for each project is located in Appendix VI of this report, along with a short summary about the project. Appendix V lists all documents and other

artifacts we determined contributed to compliance with the various standards. The numbers include some duplicate counting of single documents because components sometimes submitted one document to fulfill more than one category.

The components cited several reasons for not providing all of the documents we requested. Specifically, components said: (1) the requirement was not applicable to the investment; (2) a waiver to the requirement had been granted; (3) planning for the system pre-dated FY 2000 and the documentation was not available; (4) the system was purchased commercially off-the-shelf eliminating the need for certain processes; and (5) the investment had not reached the applicable point in the life cycle.

Figure 7 shows the number of documents we received that we determined to be responsive to our document request for each system or project.

DOJ IT Studies, Plans & Evaluations Received

Figure 7

Components	*Systems & Projects*	*Studies, Plans, & Evaluations*
ATF	NIBIN	17
BOP	ITS II	11
DEA	Concorde	15
DEA	E Com	18
DEA	EIS	20
DEA	Firebird	14
DEA	M204	8
DEA	Merlin	14
EOIR	eWorld	9
FBI	BRIDG	4
FBI	CARTSAN	11
FBI	CODIS	7
FBI	DCS	15
FBI	DCU	6
FBI	EDMS	16
FBI	FTTTF	6
FBI	IAFIS	24
FBI	IATI	18
FBI	IDW	5
FBI	LEO	9
FBI	NCIC	19
FBI	N-DEx	6
FBI	NGI	11
FBI	NICS	16
FBI	R-DEx	5
FBI	SCION	4
FBI	Sentinel	11
FBI	SMIS	21
FBI	TRP	2
FBI	TSC	8
JMD	CITP	27
JMD	IWN	23
JMD	JCON	27
JMD	LCMS	6
JMD	PKI	15
JMD	UFMS	18
ODAG	OFC	16
OJP	JGMS	12
	TOTAL	494

Source: Documents submitted by DOJ components in response to the OIG's request

Two comprehensive IT plans for the Department are required by OMB standards: the Department's IT Capital Plan and IT Strategic Plan. The IT Capital Plan, *Agency IT Investment Portfolio* (exhibit 53), was described in the second report in this series of three audits, as it represents the

Department's inventory of major IT investments. The Department's IT Strategic Plan and the component plans are described below. All other documents under the section "Studies, Plans, and Evaluations" are standards associated with each system or initiative.

The Department of Justice IT Strategic Plan

OMB Circular A-130, *Management of Federal Information Resources*, requires that federal agencies maintain strategic plans for information resources management. According to OMB, the plans should: (1) support the agency's Strategic Plan and (2) provide a description of how information resources management activities help accomplish agency missions and ensure that IT decisions are integrated with organization planning, budget, procurement, financial management, human resources management, and program decisions. DOJ Order 2880.1B, Information Resources Management Program, September 27, 2005, assigns responsibility to the CIO for developing, maintaining, and implementing the Department's IT Strategic Plan, and requires that it be aligned directly with the Department's Strategic Plan.

The *Department of Justice Information Technology Strategic Plan for 2006 – 2011*, June 2006, is designed to align IT strategic goals with the four strategic goals in the Department's Strategic Plan:

- prevent terrorism and promote America's security;
- enforce federal laws and represent the rights and interests of the American people;
- assist state, local, and tribal efforts to prevent or reduce crime and violence; and
- ensure the fair and efficient operation of the federal justice system.

To help the Department accomplish its goals, the IT Strategic Plan sets out five specific IT goals:

- enable the mission through information sharing,
- enable the mission through federated solutions,
- support effective and efficient use of IT resources,

- provide common resilient and secure infrastructure, and

- leverage common administrative solutions.

The IT Strategic Plan provides objectives for each goal and strategies for each objective. The IT goals, objectives, and strategies are intended to guide the technology capabilities toward specific outcomes. The Plan also introduces performance strategies as a means of measuring the Department's performance of objectives. The performance objectives describe, at a high level, the expected performance, while specific metrics are developed for each investment. Further, there is at least one performance measurement defined for each objective.

We reviewed the Department's IT Strategic Plan for compliance with the requirements stated in OMB Circular A-130. We found that the IT Strategic Plan supported the Department's Strategic Plan and that it contained the required description of how information resources management activities help accomplish agency missions and ensure that IT decisions are integrated with organization planning, budget, procurement, financial management, human resources management, and program decisions.

Component IT Strategic Plans

DOJ Order 2880.1B, Information Resources Management Program, allows, but does not require, components to develop their own IT strategic plans. It also requires component-specific IT strategic plans to reflect and be aligned with the strategies in the Department's IT Strategic Plan.

Five of the eight components included in this audit have developed component-specific IT Strategic Plans (ATF, BOP, DEA, EOIR, and FBI). Those IT Strategic Plans are listed in Appendix III. The Department's IT Strategic Plan was prepared by JMD.

We reviewed the IT Strategic Plans for the five components to evaluate compliance with the requirement that they be aligned with the Department's IT Strategic Plan. We found that the component IT Strategic Plans are generally consistent with the Department's Plan.

While a strategic plan is required at the Department level and components have the flexibility to develop their own strategic plans, most standards that exist related to IT studies, plans, and evaluations are applicable to individual IT systems and projects rather than to the

Department or its components. The following sections on studies, plans, and evaluations focus on the standards that apply to individual systems and projects.

IT System and Project Documents

This section presents a summary of what we obtained from components by type of document, along with a discussion of the specific standards for studies, plans, and evaluations.[18] Our approach for discussing documents in this section is generally chronological, following documents as they are produced during the development of an IT project.

We applied each document type discussed below as a test of compliance for studies, plans, or evaluations. We also assigned unique numbers to individual documents and artifacts. We prepared a matrix identifying the individual documents and artifacts we determined were responsive to our requests for studies, plans, and evaluations. Appendix IV contains the matrix of document types and systems, with identifying numbers representing individual documents that met each standard. Appendix V lists individual documents in numerical order to match with items in the matrix.

Determining compliance with the standards for studies, plans, and evaluations was complicated by variations in criteria and the long duration of many projects coupled with the fact that criteria changed over time. Determining compliance was further complicated because the components allow waivers or tailoring of the standards for each project, depending on the nature of the project. We agree that flexibility and tailoring are reasonable. As we could not perform 38 individual audits for each of the systems and initiatives in the inventory, we are providing the following discussion of compliance in terms of whether the components provided documents in a consistent manner with the generic standards we used. It was not our intent to suggest that any individual project was out of compliance at any given time, since almost no document is absolutely required. Instead, our intent was to examine how consistently the components produced certain documents specified by various criteria.

[18] This is not intended to be a comprehensive discussion of all phases or activities associated with IT projects and systems, but focuses on the tasks and documents associated with research, studies, plans, and evaluations.

Business case studies, system security plans, and PIAs are all required by criteria other than the Department's SDLC or the FBI's LCMD. Components must obtain funding for IT projects through the OMB exhibits 300, which summarize the business case, must provide system security plans in order to obtain authorization from Departmental IT security authorities to begin operating a system, and must abide by privacy laws by completing PIAs.

We found the highest levels of compliance in the areas of business case documents, which become part of the Department's annual budget process and are required to obtain funding for each system or project, and system security plans, which are required for projects to obtain the Department's authorization to operate. The components provided at least one business case document for 36 of the 38 systems in the inventory. The two exceptions, the FBI's Investigative Data Warehouse (IDW) and Secure Compartmented Information Operational Network (SCION), are included in an "umbrella" business case that represents the Department's consolidated enterprise infrastructure (CEI). The business case document represents the single document type for which we found 100 percent compliance.

System security plans also had a high level of compliance and we obtained security plans for 32 of the 38 projects. The six other projects were either too early in the life cycle for preparation of this document, or a draft security plan was undergoing review. Components also demonstrated a high level of compliance with PIAs, and we found acceptable explanations for the projects that did not submit a PIA. Components also provided project management plans for 29 of the 38 projects, and explained all but one of those exceptions.

However, we found compliance in the areas of systems engineering management, configuration management, quality assurance, validation and verification, and training plans was significantly lower.

The discussion in this section includes the numbers of whole documents we obtained that represented studies, plans, and evaluations. In the compliance matrix, Appendix IV, we included other artifacts that were submitted in lieu of, or in addition to entire documents.

Studies

Studies required by the various standards for IT activities and documents associated with each IT system or project are generally performed early in the life cycle of an IT project to identify and evaluate possible alternative solutions to meet a business need.[19] The studies include market research, alternative analyses, feasibility studies, cost-benefit analyses (or benefit-cost analyses), risk analyses, and PIAs.[20]

While the Department and DEA SDLCs specify separate documents for these studies, the FBI LCMD groups all except the PIAs into a business case document that is a virtual image of the business case section of the OMB exhibit 300 required to be submitted as part of the Department's budget. For reporting purposes, we organized the studies into groups called market/other research, business case studies, and PIAs.

As we conducted our audit, we became aware of a study that did not fit into the categories below that is related to a case management/common solution architecture for the Department. The 2004 study, sponsored by the CIO and performed by a contractor, is being used as the basis for JMD's LCMS project.[21]

Market and Other Research

The only type of research mentioned in various criteria for IT documentation is market research. The DOJ ITIM Guide specifies market research through reference to the OMB exhibit 300, *Capital Asset Plan and Business Case*. Item 1.A. of section I.E., Alternatives Analysis, of the exhibit 300 instructs agencies to discuss the market research that was conducted to identify innovative solutions for the investment. OMB's *Capital Programming Guide* indicates that federal agencies should conduct market surveillance and research to ensure that as many alternative solutions as possible are

---

[19] We grouped various documents into the category of "studies" based on the idea that a study would be a product of attempts to acquire knowledge or understanding of a subject.

[20] Privacy impact assessments (PIA) are performed later in the life cycle, after an alternative solution has been selected. The Department's SDLC places the PIA as a deliverable of the requirements analysis phase.

[21] The MITRE Corporation, *Common Solution Architecture for Case Management (the Current State), Technical Report*, April 2004.

identified for consideration once an agency need has been identified. It lists announcements, requests for information, or requests for proposals to solicit information on alternative concepts from a broad base of qualified firms. It also states that emphasis should be placed on solutions that are currently available and do not require significant development in order to minimize risk.

While market research is the only type of research specifically identified in the exhibit 300, we asked components to identify and provide any other research that had been performed in connection with their planned IT projects. Components told us there was virtually no additional IT-related research being conducted separate from the market research that is performed as part of building a business case for a system.

We requested market research from all components except the FBI because the FBI's LCMD does not specify market research independent of the business case.

Components provided 16 documents reflecting market research related to 11 of the 17 total non-FBI projects. Of the market research documents we received, the assessments included market research reports for DEA's Firebird and JMD's IWN and LCMS projects, requests for comment or information for the BOP's ITS-II and JMD's JCON, a summary report of vendor responses for JMD's UFMS, two comparative analyses of other federal systems for the ODAG's OFC, a report on public key infrastructure possibilities for the DEA's eCommerce project, and a report on digital audio recording alternatives for the EOIR's eWorld project. We obtained seven other artifacts related to market research for three projects which had also submitted documents we accepted as studies.

The 16 studies included in this discussion were separate from responses to the market research section of the *Capital Asset Plans and Business Cases* (OMB exhibits 300). Information included in the *Capital Asset Plan and Business Case* generally indicates that some market research was performed to help identify potential solutions. Six non-FBI systems were not represented by market research studies apart from the OMB exhibits 300. These six were NIBIN, Concorde, E-Commerce, M204, Merlin, and JGMS. Like the FBI projects, these six projects submitted OMB exhibits 300.

Business Case Studies

When managers decide that a system concept is worth developing further, work is performed to identify and evaluate alternative solutions. This item reflects studies performed to support the selection of a project or system and includes the following type of analyses that are frequently combined in one or two documents:

- alternatives analyses,
- feasibility studies,
- cost benefit analyses (also called benefit cost analyses), and
- risk analyses.

The Department SDLC and FBI LCMD standards vary considerably in terms of where certain types of information for these analyses should be found, but the basic information required is similar between standards. The Department and DEA SDLCs specify preparing the following:

- A feasibility study that should provide an overview of the business requirement and determination if solutions exist that are technically, economically, and operationally feasible. The feasibility study should describe and evaluate alternative solutions. The feasibility study may be documented as a separate document or as part of the cost benefit analysis.

- A cost-benefit analysis that uses the results of the feasibility study as the basis for evaluating the costs and benefits of the candidate solutions. The cost benefit analysis should additionally include a statement of assumptions made describing the present and future environment on which the analysis is based, constraints (external factors that may affect the effort), the presentation of nonrecurring and recurring costs, and an analysis of expected tangible and intangible benefits.[22] The alternative solutions evaluated should then be compared using return on investment concepts.

[22] Tangible benefits are expressed in dollars or units, such as dollars saved from streamlining transactions and saved time. Intangible benefits are normally related to mission improvements that may be difficult to quantify.

The DOJ ITIM Guide specifies a business case analysis that reflects the requirements for the *Capital Asset Plan and Business Case* (OMB exhibits 300) to summarize the results of:

- developing and evaluating alternatives;
- assessing the relative risks and mitigation strategies;
- performing a return on investment (ROI) analysis, including a benefits cost analysis;
- developing performance measures and indicators;
- addressing security and privacy issues; and
- selecting the best alternative based on ROI, risk mitigation, benefits cost analysis, and other performance measures.

The FBI LCMD specifies an initial and a final business case that is virtually identical to the requirements for the OMB exhibit 300.

This audit generally reports on documents the components provided in response to our requests for specific documents. One exception to this is for business case studies. Some components submitted the OMB exhibit 300, *Capital Asset Plan and Business Case,* in response to this request, but many did not. Therefore, we obtained a number of additional exhibits 300 from other sources and have credited them to this test regardless of how the component responded to the document request.

Overall, we obtained 46 documents we categorized as a business case study, including at least one for 36 of the 38 systems or projects. The 46 business case studies include multiple documents for 9 projects. Several components submitted more than one OMB exhibit 300, representing multiple budget years, but we counted multiple OMB exhibits 300 for each project as one document. Additional studies we obtained included Alternatives Analyses and Cost Benefit Analyses.

We did not receive a business case study for the FBI's Investigative Data Warehouse (IDW) or Secure Compartmented Information Operational Network (SCION) projects because they are included in an OMB exhibit 300 for the "comprehensive enterprise infrastructure" for the Department.

Additionally, we obtained more than 70 other artifacts related to business cases, including feasibility statements, mission needs statements, concept of operations documents, and cost benefit analysis spreadsheets.

Overall, we found the highest level of compliance with standards in the area of business case studies. The budget requirement for the OMB exhibit 300 undoubtedly contributes to the high level of compliance, as the case study is needed to obtain funding as part of the budget process.

Privacy Impact Assessments

PIAs are required by DOJ Order 2880.1b to ensure the Department reviews the potential impacts on individuals' privacy concerns that may result from the development and use of computer-based information systems that collect or store personal data about individuals. All components are required to conduct a PIA for any new information system that contains sensitive information about individuals, uses new techniques to manipulate existing data about individuals in a way that such data is readily retrievable, or collects and maintains personal information about individuals that has not previously been collected and maintained by the component. JMD is responsible for enforcing compliance with this policy through the Department's ITIM process.

The DOJ ITIM Guide instructs components to address privacy issues in developing the business case, in preparing the *Capital Asset Plan and Business Case*, and when preparing a disposal plan. The DOJ and DEA SDLC*s* require the PIA to be performed as part of the requirements analysis phase of a system's life cycle.

The DOJ SDLC defines a PIA as a written evaluation of the impact that the implementation of the proposed system would have on privacy. Guidance for preparing a PIA is provided on the Department's intranet, and consists of a list of questions to be answered about data in the system and the impact of the system on privacy. The assessment begins with a privacy threshold analysis to determine whether there is a need for a full PIA for each system.

Compliance with the PIA requirements appears consistent. We obtained 33 PIAs and privacy threshold analyses for 23 of the 38 systems and projects in the revised inventory, with some components submitting separate PIAs for different functions or modules of a system. PIAs were not required for every project. The threshold analyses for NIBIN and PKI determined there was no need for a full PIA for those systems, and we

obtained an initial or full PIA for the other 21 of the 23 systems and projects.

We did not obtain PIAs or threshold analyses for 15 systems or projects. DOJ Order 3011.1A, Compliance with the Privacy Requirements of the Privacy Act, the E-Government Act, and the FISMA, March 6, 2007, states that PIAs identifying how information in identifiable form is collected, stored, protected, shared, and managed in an IT system or online information collection are required when developing or procuring new technology or making substantial modifications to existing technology. This would exempt older systems that have not undergone significant modification in the way described. Although the scope of this audit did not include evaluating information about modifications to all of the older systems in the inventory, this order would appear to exempt 7 of the remaining 15 systems: the DEA's M204 corporate systems, the FBI's DCU, IAFIS, LEO, NCIC, NICS, and R-DEx.

The DEA responded that a PIA was too broad for the infrastructure project Firebird and not applicable to Merlin, which is also an infrastructure project. The FBI told us that the PIAs for the FTTTF and TSC existed, but did not provide them to us. We did not obtain PIAs or explanations for the FBI's IDW or TRP. The TRP is, however, at the beginning of its life cycle and is not yet at the phase of the FBI's LCMD that requires a PIA. JMD told us that the PIA for IWN was not completed yet, and OJP responded to this item for the JGMS with its certification and accreditation plan of actions and milestones.

Plans

The plans specified by the DOJ and DEA SDLCs for each IT system or project include many types of plans that are developed after an alternative solution has been selected. These plans include:

- risk management,
- acquisition,
- project management,
- system security,
- systems engineering management,
- configuration management,
- quality assurance,
- validation and verification,
- test,
- conversion,
- implementation,

- training,
- contingency, and
- disposition.

The FBI LCMD also requires many of the same plans, but uses different names for some. Each of the differences is described below.

Risk Management Plans

The SDLCs specify risk management plans to be prepared during the system concept development phase, along with the feasibility and cost benefit studies. The risk management plan documents the results of assessing and planning to manage programmatic and technical risks of the system or project. The plan should identify and assess risks, and detail the strategies that will be employed to mitigate the risks.

The DOJ ITIM Guide describes assessing risk as part of analyzing alternatives, and reporting such risk assessment in the *Capital Asset Plan and Business Case* (OMB exhibit 300). When completing the exhibit 300, agencies are instructed to assess various risks, including those associated with schedule, initial costs, life-cycle costs, technical obsolescence, risk of monopoly, capability of the agency to manage the investment, overall risk of investment failure, security, privacy, and project resources.

Components provided 32 risk management plans for 25 of the 38 systems and projects. A number of components submitted the OMB exhibit 300 or other artifacts as their risk management plans. While the exhibit 300 contains information on risk management, it also requests the date of the risk management plan, suggesting that an independent plan should exist. We included artifacts, such as information from the OMB exhibit 300, in the compliance matrix, but did not count these as a risk management plan.

In addition to the OMB exhibits 300, other artifacts included risk registers, which are spreadsheets listing risks and mitigation strategies, risk analyses, and risk management sections of other documents, such as project plans. The number of projects represented by either risk management plans or other artifacts was 33 of the 38 projects. Five projects did not provide any specific response to this request, but Firebird, IAFIS, NICS, and TRP all submitted OMB exhibits 300 that included a risk management section. SCION, the final system, is included in the Department's consolidated enterprise infrastructure OMB exhibit 300.

Acquisition Plans

The SDLCs specify preparation of an acquisition plan during the planning phase of a system life-cycle. This plan should document how all government resources and contractor support services will be acquired during the life of the project. Acquisition plans are specified in the DOJ ITIM Guide and also are included in the final business case under current FBI standards. We did not request acquisition plans from the FBI, as FBI officials told us the acquisition plans are in the business case. As is discussed in the section on business case studies, the FBI was compliant with business case studies. However, we did obtain two documents related to acquisition planning for the FBI's Sentinel project.

Other components provided acquisition plans or some relevant alternate documentation for 13 of the 17 non-FBI systems and projects in the revised inventory. Alternate documentation included justification for other than full and open competition and the acquisition section of *Capital Asset Plans and Business Cases*, which summarizes the acquisition strategy. We obtained OMB exhibits 300 for all of the other non-FBI projects that did not provide separate acquisition plans. While the other components did not suggest that the OMB exhibit 300 fulfilled the requirement for an acquisition plan, we accepted them as such in order to ensure similar treatment to the FBI projects. However, we do not identify this as an area of high compliance because the OMB exhibit 300 clearly expects that components will develop a separate acquisition plan.

Project Management Plans

The SDLCs indicate that project management plans should be prepared for all projects. The plans are intended to document project scope, tasks, schedule, allocated resources, and interrelationships with other projects. The plans also provide details on the involved functional units, required job tasks, cost and schedule performance measurement, and milestone and review scheduling. Revisions to the project management plan should occur at the end of each phase and as information becomes available. The project management plan should reflect the entire scope of what is to be accomplished. Project management plans are also specified in the DOJ ITIM Guide.

Components provided 44 project management plans for 29 systems and projects, and 42 other artifacts representing 28 projects, together representing a total of 31 of the 38 projects. We included artifacts in the

compliance matrix in Appendix IV. Common artifacts submitted in relation to this plan were schedules of tasks and work breakdown structures.

We did not obtain project plans or relevant artifacts for seven projects, four of which predated the FBI's implementation of its LCMD (IAFIS, LEO, NICS, and R-DEx). We did not receive an explanation for why no project management plans for the FBI's SCION and TRP were provided. In addition, the ATF waived compliance to the SDLC for its NIBIN system "due to the nature of the contract and special contractual constraints whereby the Contractor provides for 100% of the necessary customer support and maintenance support required to install, configure, implement and sustain all IBIS systems (hardware and software)."

System Security Plans

The various business and law enforcement functions within the Department depend on the confidentiality, integrity, and availability of systems and data. The DOJ SDLC specifies that system security plans should contain information about the system environment, information sharing, sensitivity of information processed, management controls, security controls, operational controls, contingency planning, security training, audit trails, and access controls.

The Department requires that all IT systems pass a security Certification and Accreditation process that is intended to ensure the adequacy of computer system security. Security plans and successful security test results are needed to obtain the Department's authorization to operate. This likely ensures that system security plans and related security tests are among the most reliably prepared documents in the IT development process.

Components provided 40 system security plans and 33 other relevant artifacts for 32 systems. Included as artifacts in the compliance matrix in Appendix IV are items such as security sections of project management plans, authorizations to operate, and other artifacts of the certification and accreditation process. Of the six projects not represented here, the FBI and JMD told us the plans for NGI, Sentinel, and LCMS did not yet exist, which was reasonable given the status of the projects at the time of our field work. We were also informed that the draft security plan for the FTTTF was being reviewed at the time of our field work. We did not obtain a plan or an explanation from the FBI regarding the BRIDG or TRP projects. Overall, we found compliance with this system security standard extremely high.

Systems Engineering Management Plans

According to the Department's SDLC, the systems engineering management plan (SEMP) should be developed during the planning phase of IT project development. The SEMP is intended to document the strategy for executing the technical management aspects of the project, and should include information about responsibilities for the technical effort, technical processes, and procedures to be applied. It should address control strategies for data management, technical performance measurement, interface management, and formal and informal technical reviews. The FBI's LCMD also specifies SEMPs.

In response to our request, components provided only 11 SEMPs and 6 relevant artifacts for 13 projects. Components did not submit items we accepted as SEMPs for 25 of the 38 IT projects. In addition to the NIBIN contract waiver, components told us the SEMPs had not yet been developed or were not applicable for their projects. Others submitted project management plans or concept of operations documents to meet this requirement, but we did not accept the brief descriptions included in these documents for this test.

Configuration Management Plans

According to the DOJ SDLC, configuration management plans document uniform practice for managing system software, hardware, and documentation changes throughout a development project. The FBI LCMD also specifies configuration management plans.

Components provided 28 configuration management plans and 5 related artifacts for 26 projects. The 12 projects not submitting configuration management plans were NIBIN, ITS-II, BRIDG, CODIS, DCU, FTTTF, IDW, N-DEx, R-DEx, TRP, TSC, and OFC. In addition to the NIBIN contract waiver, component explanations for not submitting this item included that the documents had not yet been developed or the standard was not applicable.[23]

[23] It was beyond the scope of this audit to determine what was appropriate for each project for every type of study, plan, or evaluation that may be prepared for individual projects.

Quality Assurance Plans

The DOJ SDLC indicates the purpose of quality assurance plans is to ensure that delivered products satisfy contractual agreements, meet or exceed quality standards, and comply with approved processes. The plans should include an overview of the processes to ensure that processes and products associated with hardware, software, and documentation are monitored, sampled, and audited to ensure compliance with methodology, policy, and standards.

Components provided 17 quality assurance plans for 16 projects.[24] We included 12 other relevant artifacts for 5 projects in the compliance matrix, representing a total of 20 projects. No quality assurance plans or related artifacts were obtained for 18 of the 38 projects. The 18 projects were: NIBIN, ITS-II, BRIDG, CODIS, DCS, DCU, EDMS, FTTTF, IDW, LEO, NCIC, N-DEx, R-DEx, SCION, TRP, TSC, CITP, and JGMS. In addition to the NIBIN contract waiver, component explanations for not submitting this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Validation and Verification Plans

Validation and verification plans describe the testing strategies that will be used throughout a project's life-cycle phases. Such plans should include descriptions of contractor, government, and appropriate independent assessments required by the project. They should also reflect the major reviews that will be performed through the project. However, the SDLC does not require that any validation and verification be performed independently.

The FBI LCMD also requires this plan and defines verification and validation as a disciplined approach to assessing software products throughout the software development life cycle to ensure that quality is built into the software and that the software satisfies business functional requirements. Verification and validation employs review, analysis, and testing techniques to determine whether a software product and its intermediate deliverables comply with business functional requirements and quality attributes. The LCMD specifically defines verification as the process

[24] This number includes one quality management plan counted five times because it is being used for five DEA projects (Item #83).

of determining whether products in a given phase of the development process fulfill the requirements established during the previous phase and validation as the process of evaluating software at the end of the software development process to ensure compliance to software requirements.

Components provided 8 validation and verification plans and 14 other related artifacts for 10 projects. We accepted test plans in response to this document request for three projects. In our judgment, verification and validation plans should include more than software testing. Requirements and design products should also be subject to verification and validation. The ten projects we determined responded to this item were: DEA's E-Commerce, EIS, Merlin, and M204, the FBI's IAFIS and TSC, JMD's CITP, IWN, and JCON, and OJP's JGMS. The other 28 projects did not provide a validation and verification plan or we did not accept minimal test documentation that was submitted in response to this request. In addition to the NIBIN contract waiver, component explanations for not submitting this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Test Plans

Both the SDLC and FBI LCMD specify test master plans that should document the scope, content, methodology, sequence, management of, and responsibilities for test activities. The testing should include integration, system, user acceptance, and security testing.

Components provided 51 test plans and 19 other related artifacts for 30 projects. These represent plans for different types of testing and testing of various modules or functions of the same system such as security, acceptance, functional, maintainability, report generation, and integration tests. Of the eight projects not represented, three had not reached the appropriate stage of the life cycle for this document: CODIS-Next Generation project, NGI, and LCMS.[25] Of the remaining five projects, only ITS-II responded that the item was not applicable. There were no specific responses on the other four projects (BRIDG, IDW, SCION, and TRP).

[25] It was beyond the scope of this audit to ensure that we obtained test plans for every appropriate module, phase, or function of each project. We are reporting what we obtained in response to the request for studies, plans, and evaluations.

Conversion Plans

The SDLC calls for conversion plans to be prepared during the design phase of the life cycle to document the results of design work on conversion and transition strategies if information needs to be converted or migrated to the new system. The plans should describe the strategies involved in converting data from the existing to the new environment. Because the FBI's LCMD requires transition plans to include data conversion issues, we requested transition plans for the FBI projects.

Components provided 13 conversion and transition plans for 10 projects. Most of these were FBI transition plans, although JMD submitted conversion plans for the Classified Information Technology Program (CITP) and Unified Financial Management System (UFMS) projects, the BOP submitted a plan for ITS-II, and JMD submitted two related artifacts for JCON. In addition to the NIBIN contract waiver, component explanations for not submitting this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Implementation Plans

According to the SDLC, implementation plans are to be prepared during the design phase to describe how the system will be deployed, installed, and transitioned into an operational status. The FBI LCMD refers to its comparable plan as an installation plan.

Components provided 29 implementation, deployment, or installation plans and 21 other related artifacts for 24 projects. Component explanations for the 14 other projects not represented in this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Training Plans

The SDLC also calls for training plans to be prepared during the design phase. The training plan should outline the objectives, needs, strategy, and curriculum to be addressed when training users on the new or enhanced information system. The training plan should present the activities needed to support the development of training materials, coordination of training schedules, reservation of personnel and facilities, and other training-related tasks.

Components provided 16 training plans and 5 other relevant artifacts for 19 projects. Component explanations for the 19 other projects not represented in this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Contingency and Continuity of Operations Plans

The DOJ SDLC specifies contingency planning as a function of the development phase of a system's life cycle. The SDLC cites OMB A-130 as requiring the preparation of plans for general support systems and major applications to ensure continuity of operations. The purpose is to provide for the continuation of critical mission and business functions in the event of disruptions. The plans are known by various names, such as disaster recovery, continuity of operations, or contingency plans.

We obtained 23 contingency plans or continuity of operations plans and 1 related artifact for 19 projects. Component explanations for the 19 other projects not represented in this item included that the documents had not yet been developed or were not applicable.

Disposition Plans

Disposition plans are intended to end the operation of a system in a planned, orderly manner and to ensure that system components and data are properly archived or incorporated into other systems. The plan should be developed during the disposition phase, according to the SDLC, which begins when a decision is made to terminate or replace a system.

Components provided one disposition plan for JMD's PKI and one other related artifact for the FBI's DCU. The PKI document was prepared early in the PKI life cycle. It was our understanding that the DEA's M204 corporate systems and the BOP's ITS-II were both nearing the end of their life cycles, but other systems in the revised inventory were not yet at that stage.

Evaluations

During our field work for this audit, we requested IT project test reports, ongoing reviews of project status, and earned value management (EVM) reports to obtain information to describe IT planning problems within the Department. We obtained 42 test reports and 25 other relevant artifacts for 24 projects. We also obtained 86 documents and other related artifacts for 25 projects that we categorized as ongoing performance evaluations. These items included Dashboard reports to the OCIO, EVM spreadsheets, project reviews, results of gate reviews for FBI projects, project status reports, briefings for component and Departmental managers, and lessons learned statements. We found that most of these materials presented status information needed for project management and decision-making, but were not necessarily directed at describing planning problems. These items are included in the compliance matrix and list of unique documents in appendices IV and V.

To obtain information about the effectiveness of system development and acquisition efforts, we have limited our assessment of evaluations in this audit report to full reports produced about problems experienced during projects, or reports about systems and projects following implementation of the system. We requested post-implementation review reports, which include in-process review reports and user satisfaction review reports.

Post-Implementation Review Reports

According to the SDLC, post-implementation reviews are conducted after a system has been in production for a period of time and are used to evaluate the effectiveness of the system development. The review should determine whether the system does what it was designed to do, supports users as required, and was successful in terms of functionality, performance, and cost benefit. It should also assess the effectiveness of the development activities that produced the system. The review results should be used to strengthen the systems as well as the component's system development procedures.

In-process reviews are performed during operations and maintenance to assess system performance and user satisfaction, and should occur repeatedly after a system has been implemented to ensure the system continues to meet needs and perform effectively.

The FBI LCMD does not require a post-implementation review as such. However, it does specify annual project-level operational reviews that are

conducted by the operations and maintenance organization to ensure that the fielded system is continuing to support its intended mission and can be continuously supported, operated, and maintained in the future in a cost-effective manner. The FBI LCMD also calls for acceptance reviews at the time of implementation.

Components provided seven post-implementation reports and six other relevant artifacts for ten projects. These are discussed in Finding 2 of this report. Component explanations for the 28 other projects not represented in this item included that the documents had not yet been developed, were not applicable, or were no longer available if they were developed several years ago.

Conclusion

We found the highest levels of compliance with studies, plans, and evaluations in the areas of business case documents, which become part of the Department's annual budget process and are required to obtain funding for each system or project, and security plans, which are required for projects to obtain authorization to operate. The components provided at least one business case document for 36 of the 38 systems in the inventory. The two exceptions, the FBI's Investigative Data Warehouse (IDW) and Secure Compartmented Information Operational Network (SCION), are included in an "umbrella" business case that represents the Department's consolidated enterprise infrastructure (CEI). The business case document is the single document type for which we found 100 percent compliance.

System security plans also had a high level of compliance and we obtained security plans for 32 of the 38 projects. The six other projects were either too early in the life cycle for preparation of this document, or a draft security plan was undergoing review. Components also demonstrated a high level of compliance with PIAs, and we found acceptable explanations for the projects that did not submit a PIA. Components also provided project management plans for 29 of the 38 projects, and explained all but one of those exceptions.

However, we found compliance in the areas of systems engineering management, configuration management, quality assurance, validation and verification, and training plans was significantly lower.

Departmental oversight is designed to focus on the Capital Planning and Investment Control process for selecting and prioritizing IT investments. It is not designed to enforce policies and procedures on IT project

documentation.[26] Department-level oversight of individual IT projects is performed through presentations to the Departmental Investment Review Board, the CIO's Dashboard report, and through the OMB exhibit 300s, all of which are described in the second report in this series. This oversight includes tracking of actual performance against scheduled milestones and costs, but does not involve JMD officials in the details of IT documentation for individual projects.

Based on the limited number of plans and evaluations produced on these major systems and projects, the CIO should evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects.

Recommendations

We recommend that the Department's CIO:

1. Evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects.

2. Consider revising the guidelines for tailoring the work pattern for specific types of projects.

[26] The CIO does have specific responsibilities to enforce security standards.

Finding 2: IT Planning Problems

Prior OIG reports have identified IT planning problems that resulted in terminated projects, delays in implementation, cost increases, and problems with system data. Significant problems in planning that have been identified include weaknesses in contract management, business process re-engineering (BPR) and defining system requirements, and coordination between federal agencies. We originally planned to use evaluations we obtained from components to identify problems the Department has experienced in planning for IT systems. However, components have produced few meaningful evaluations of project management for either successful or failed IT projects. Therefore, we reviewed prior OIG reports and sought other reports performed or sponsored by the Department that identified IT planning problems.

To identify problems the Department has experienced in planning for IT systems and projects, we reviewed previous OIG audit and inspection reports. We used OIG performance audits, financial statement audits, information technology security audits, and inspections to help identify the scope of problems the Department has experienced in IT planning. The focus of the audits and reviews varied and included general IT management, the management and progress of individual IT projects, the performance of individual systems following implementation, system security, and system controls. The OIG reports we reviewed are listed in Appendix VII. We also reviewed special reports prepared for the FBI on the terminated VCF project.

The overall objective for the IT standards described in the Introduction to this report is to improve the acquisition, use, and disposal of information technology by the federal government so as to improve the productivity, efficiency, and effectiveness of federal programs. Prior OIG reports have identified IT planning problems that resulted in terminated efforts, implementation delays, problems with data in implemented systems, and cost overruns.[27] The OIG reports described causes for the terminations, delays, and other problems that include weaknesses in contract management, project scheduling, BPR, requirements definition, and cooperation between federal agencies.

[27] Some of the systems and initiatives included in this analysis were not included in the revised inventory but were the subject of OIG reports. All of the systems and initiatives in the revised inventory used for this audit either were implemented or are currently in development.

During this audit we looked for any IT projects that had either failed or been terminated, such as the FBI's VCF and LIMS projects discussed below. The OIG found during work on the second report in this series that a prior effort on JMD's Justice Consolidated Office Network (JCON) project had been terminated before beginning the current project in FY 2001. JMD, however, was not able to provide an evaluation of the failure. In our opinion, failure to evaluate why a contract failed suggests a serious gap in evaluating project management practices. We believe that troubled and terminated projects should be evaluated to determine the causes of the problems.

Business Process Re-engineering and Requirements Weaknesses

The DOJ SDLC indicates that BPR should be the underpinning of any new system development or initiative as part of strategic planning for information systems, and that agencies should consider BPR before requesting funding for a new project or system development effort. BPR is defined as the redesign of the organization, culture, and business processes using technology as an enabler to achieve significant improvements in cost, time, service, and quality. The results of successful BPR are increased productivity and quality improvements.

The FBI's effort to develop a case management system to replace its obsolete Automated Case Support system has been subject to project restarts or continuations with new titles twice since its initiation.[28] The first effort, undertaken in mid-2001 as the User Applications Component of the Trilogy project, was originally scheduled to be implemented in 2004. This effort was never implemented because the vision and functional requirements for the system changed significantly during the project. After the attacks of September 11, 2001, and other events affecting the FBI, the vision for the system changed from one that would simply consolidate existing applications to one that would implement a new overall workflow process for FBI agents, analysts, and support personnel.

[28] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project,* Audit Report 05-07, February 2005.

The effort subsequently became the Virtual Case File (VCF) project. The VCF was intended to make criminal and terrorist investigation information readily accessible throughout the FBI. However, the FBI did not accept an initial delivery from the contractor in December 2003 because the system was not fully functional and did not meet FBI requirements. Subsequent deliveries did not occur because of difficulties experienced in completing the initial version of the VCF. The FBI told auditors that subsequent deliveries were not being pursued given the problems in the first delivery. The OIG report on the VCF project stated that one of the most significant problems with managing the schedule, cost, and technical aspects of Trilogy was the lack of a firm understanding of the design requirements by both the FBI and contractors. During the initial years of the project, the FBI had no firm design baseline or roadmap for Trilogy. According to one FBI official, Trilogy's scope grew by about 80 percent from the initiation of the project. The FBI terminated the VCF portion of Trilogy in March 2005 after spending $170 million because of the lack of progress on its development and concerns that the development environment would make the system difficult to enhance and maintain. As discussed in two OIG audit reports, the effort has been re-started as the $425 million Sentinel project, which is scheduled for completion in December 2009.[29]

A contracted study of the FBI's terminated Virtual Case File project found that the original plans for the case management portion of the Trilogy project were not based on a new vision of how the FBI could use IT to transform the way it performs its mission. Specifically, the unpublished report indicated that senior managers were not involved in efforts to re-engineer business processes or in rethinking the FBI's use of IT, and that while users working on the re-engineering were experienced agents, none had experience with complex IT development projects or business process re-engineering.

---

[29] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System,* Audit Report 06-14, March 2006.

and

Department of Justice, Office of the Inspector General, *Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System,* Audit Report 07-03, December 2006.

Another terminated project at the FBI was an initiative to implement a new Laboratory Information Management System (LIMS) to replace its Evidence Control System, which was originally created in 1978.[30] The LIMS contract was awarded in September 2003, was initially supposed to be implemented within 90 days of contract activation, and was terminated in January 2006 due to concerns over security requirements. According to an OIG audit, the project failed because of problems meeting the FBI's security requirements and because of delays in implementing a web-browser interface.

The OIG determined that specific security requirements for the system were defined late in the project, hindering the contractor's ability to comply. The LIMS Request for Proposals (RFP) had required security to be part of the system, but the FBI strengthened its security requirements after the contract award in response to high-profile espionage-related security breaches in the FBI. The audit found that the FBI had failed to document security requirements adequately and, to the extent the security requirements evolved, did not clarify those changes through contract modifications.

Cooperation Between Agencies

OIG audits and reviews have also identified difficulties when the Department attempts to work with other agencies to develop and implement successful IT systems. For example, lack of cooperation has cost time in the effort to coordinate fingerprint sharing between the Department and the Department of Homeland Security (DHS). Similar problems threaten the success of the Secure Flight Program and the Integrated Wireless Network (IWN).

The OIG audit of the Terrorist Screening Center's (TSC) efforts to support the Department of Homeland Security's (DHS) Secure Flight Program found that the TSC had been hindered and delayed in its efforts to prepare for implementation by the DHS-led Transportation Security Administration's failure to make, communicate, and comply with key program and policy decisions in a timely manner.[31] In addition to perceived

[30] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Implementation of the Laboratory Information Management System,* Audit Report 06-33, June 2006.

[31] Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, Audit Report 05-34, August 2005. Redacted

problems in planning at DHS, cooperation between the TSC and DHS has been weak.

The OIG has performed a series of reviews of the FBI's progress toward achieving interoperable fingerprint identification systems with federal immigration authorities.[32] Since 1999 JMD has maintained oversight of the integration of the FBI's fingerprint identification system, Integrated Automated Fingerprint Identification System (IAFIS), and the Department of Homeland Security's Automated Biometric Identification system, IDENT. The 2001 USA Patriot Act and the 2002 Border Security Act both set requirements for a data system that would allow sharing of identification information in federal law enforcement databases with immigration authorities to determine whether to allow aliens to enter the United States.

Differences between the FBI and the DHS over the number (2 or 10) and type of fingerprints (flat or rolled) to be collected held up progress in this area. DHS deployed an additional system in 2004, US-VISIT, which uses IDENT to collect fingerprints, and is also used by Department of State employees at visa-issuing consulates. The principal barriers to achieving interoperability identified in an OIG December 2004 report were the different fingerprint collection requirements of the two agencies, and disagreement on the details of how to make information readily accessible to federal, state, and local law enforcement agencies. The most recent OIG report on the fingerprint integration issue indicated that the first barrier was resolved by DHS' May 2005 decision to implement a 10-print standard. Currently, efforts are underway to make IAFIS, IDENT, and US-VISIT fully interoperable by December 2009.

The OIG recently released an audit report on the Integrated Wireless Network (IWN) project that is intended to enhance the ability of federal law enforcement agencies in the Departments of Justice, Homeland Security, and Treasury to communicate with each other.[33] IWN would also allow interoperability with state and local law enforcement partners and meet mandates to use federal radio frequency spectrum more efficiently. The OIG's audit found that the project, which may cost $5 billion, is at high risk

---

[32] Department of Justice, Office of the Inspector General, *Follow-up Review of the FBI's Progress Toward Biometric Interoperability Between IAFIS and IDENT,* Inspections Report I-2006-007, July 2006, is the most recent report in the series of six reports.

[33] Department of Justice, Office of the Inspector General, *Progress Report on Development of the Integrated Wireless Network in the Department of Justice,* Audit Report 07-25, March 2007.

of failing to deploy an integrated wireless network for use by the three federal departments. The reasons include a fractured IWN partnership, lack of an effective governing structure for the project, and disparate departmental funding mechanisms that allow the departments to pursue separate wireless communications solutions apart from IWN.

Contract Management Weaknesses

The OIG conducted an audit of the FBI's Trilogy project to assess the FBI's progress in meeting cost, schedule, technical, and performance targets for the three components of Trilogy.[34] The OIG found that the VCF portion of the Trilogy project significantly exceeded the original schedule and budget. In addition, the FBI received an additional $78 million to accelerate the infrastructure and communications portions of the Trilogy project. Those segments were completed by April 2004, only one month before the original target date of May 2004. The audit found that while the Trilogy project had succeeded in improving the FBI's IT infrastructure and communications capabilities, the new case management system was incomplete and would not meet the FBI's needs. The OIG recommended the FBI monitor its Enterprise Architecture and apply ITIM processes to improve the FBI's ability to identify, select, and manage future IT projects. Since then, the FBI has implemented a formal project management and oversight methodology, its Life Cycle Management Directive (LCMD), to address these weaknesses and the LCMD is being used in the current Sentinel project.[35]

The OIG examined the LIMS project and found that firmly managed schedule, cost, technical, and performance benchmarks would have raised warning signs earlier in the project. The LIMS contract was awarded 14 months before the FBI implemented its LCMD, a critical initiative that provided the FBI with a structured IT investment management process. The LCMD also involves project oversight at the enterprise level. In the LIMS audit, the OIG made recommendations to consider whether an existing commercial off-the-shelf system would meet the FBI's needs, ensure that any future laboratory information system follows the FBI's LCMD processes

---

[34] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project,* Audit Report 05-07, February 2005.

[35] The FBI's LCMD methodology is fully documented in U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Pre-Acquisition Planning for and Controls Over the Sentinel Case Management System*, Audit Report 06-14, March 2006.

and is overseen by an experienced IT project manager, and establish controls to ensure that expenses are not incurred prematurely in the development of a successor project.

During its annual financial statement audit, the OIG identified inadequate oversight of contract staff as a weakness in financial statement audits, specifically at OJP.[36] The OIG audit found that OJP contractors do not consistently adhere to Department policies and procedures for managing system changes and do not consistently provide OJP management with necessary technical and logistical information for production systems. As a result, OJP management is unaware of system operational information and system modifications implemented by the contractors. The OIG concluded that the OJP CIO needed to improve his oversight and monitoring of contractor activities in order to reduce the risk of negative effects on OJP operations and financial data.

IT Program Management

The OIG audit of JMD's Joint Automated Booking System (JABS) found that booking stations installed at Bureau of Prisons (BOP) facilities were brought online in April 2004, 2 years after the equipment was installed during the summer of 2002.[37] According to JMD officials, the software that was originally installed with the equipment had major problems that were not discovered until after all 240 JABS workstations had been installed. The 2-year delay in implementing JABS at the BOP was caused by inadequate oversight of the contractor's work.

Since then, in audit reports issued in 2004 and 2005, the OIG found that the Department has begun to improve its oversight and guidance of the components' EA and ITIM processes on Department-developed frameworks.[38] In its audit of the *Status of Enterprise Architecture and Information Technology Investment Management in the Department of Justice*, the OIG made recommendations for improving the Department's IT

---

[36] U.S. Department of Justice, Office of the Inspector General, *Office of Justice Programs Annual Financial Statement Fiscal Year 2006,* Audit Report 07-21, March 2007.

[37] U.S. Department of Justice, Office of the Inspector General, *The Joint Automated Booking System,* Audit Report 05-22, May 2005.

[38] Department of Justice, Office of the Inspector General, *The Status of Enterprise Architecture and Information Technology Investment Management in the Department of Justice,* Audit Report 06-02, November 2005.

management, including completing the Department-wide Enterprise Architecture, providing guidance to components for the development and maintenance of EAs, ensuring that components requiring ITIM processes develop them, and establishing a clear schedule for completing the ITIM framework and a mature ITIM process.

In another audit, the OIG found the DEA had made significant progress in managing its EA and the ITIM processes.[39] Although the DEA had not yet developed a target EA or developed a transition plan to accomplish its target, it had established a foundation by developing an overview of its existing IT structure. The DEA also assigned roles, committed resources, and established a plan to complete its target architecture. When the EA is complete, the DEA will be able to better manage current and future IT infrastructure and applications.

The OIG's first in a series of audits examining Sentinel evaluated its development and implementation by reviewing the management processes and controls the FBI applied to the pre-acquisition phase of Sentinel.[40] The OIG found that the FBI established ITIM processes through its Life Cycle Management Directive (LCMD) and was working to fully define its enterprise architecture. If followed, the FBI's new IT management processes, reviews, and controls, coupled with external oversight by the OIG, contractors, congressional committees, and others, should help the FBI identify and minimize failures to achieve cost, schedule, performance, and technical benchmarks for the Sentinel project.

The OIG review of the TSC identified numerous problems with data in the database that is used for screening persons from consolidated terrorist-related watch lists, most of which resulted from the urgency with which the consolidated database was implemented.[41] The data problems included incomplete, missing, and inaccurate information in records, and duplicate records containing inconsistent information. The potential effects of these

---

[39] Department of Justice, Office of the Inspector General, *The Drug Enforcement Administration's Management of Enterprise Architecture and Information Technology Investments,* Audit Report 04-36, September 2004.

[40] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System*, Audit Report 06-14, March 2006.

[41] Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005. (Limited Official Use and Redacted)

data integrity problems include the possibility that screeners may not identify known terrorists during screening. The OIG found that these were caused by a lack of strategic planning, weak planning due to the pressure to implement a system, and user training weaknesses. The OIG is currently performing a follow-up review on the accuracy of the TSC watchlist.

Post-Implementation Evaluations

We originally planned to use evaluations we obtained from components to identify problems the Department has experienced in planning for its IT systems. However, this proved impossible because the Department has produced few meaningful evaluations of project management for either successful or failed IT projects, with the exception of two terminated projects in the FBI.

According to the DOJ SDLC, one purpose of post-implementation reviews is to assess the effectiveness of the life-cycle development activities that produced the system. This includes analyzing if proper limits were established in the feasibility study and if they were maintained during implementation, addressing the reasons for variances between planned and realized benefits, addressing the reasons for differences between estimated and actual costs, and evaluating whether training was adequate, appropriate, and timely. The review results are intended to be used to strengthen the system development procedures as well as the system itself.

The DOJ ITIM Guide calls for continuous monitoring of investments to assess progress against established cost, schedule, and performance metrics in order to mitigate any risks or costs on an on-going basis. The ITIM Guide also indicates that the activities of the evaluation phase include applying lessons learned from post-implementation reviews and periodic operational analyses for ITIM process improvement. The lessons learned for ITIM process should be incorporated into the select and control phases for future IT investments.

We reviewed the seven post-implementation review reports we obtained, four of which did not contain information on lessons learned in project management. The reports included two classified project closeout reports on two phases of one project. According to one of the reports, one phase was accomplished on schedule and within budget and included no lessons learned or discussion of any problems. The other report contained two lessons learned that were marked as unclassified. The lessons were:

- The adequacy of contractor performance was directly related to the level of oversight and attention-to-detail by the government team. The recommendation associated with this lesson was to schedule face-to-face meetings with the contractor and maintain that schedule.

- The initial budget for the program did not include all necessary costs to support external customers. The recommendation was to use an independent government cost estimate to determine whether the contractor's proposed price/cost is reasonable.

JMD's JCON project has produced two reports of lessons learned on the implementation of JCON in two components. The report on JCON implementation in the Civil Division described the need for better definition of project milestones and performance indicators to improve communications and develop a shared perspective on project performance. It also identified needs: (1) to devote greater attention and resources to quality review of deliverables and other work products, (2) for closer and more detailed review of requirements and design phase documentation, and (3) for improved adherence to change control procedures. The report on JCON implementation in the Civil Rights Division identified opportunities for improvement in the areas of communication and thoroughness of design. Comments in the report noted that requirements gathering needed to be as good as possible to avoid problems with design and implementation.

In addition, an assessment against project performance metrics was performed for one portion of the DEA's E-Commerce project. The evaluation provided performance data, but no lessons learned information about project management.

In light of the limited number and scope of evaluations of project management, the Department should ensure that post-implementation evaluations and post-termination evaluations of IT projects are performed so lessons learned can be incorporated into the Department's standards and used to improve project management on future projects.

Conclusion

Prior OIG reports have identified planning problems on individual systems and projects that include weaknesses in business process re-engineering, requirements planning, cooperation between agencies, and IT program and contract management. These weaknesses have contributed to:

- project re-starts, cost increases, and delays in implementation of the FBI's case management system;
- termination of the FBI's LIMS project;
- delays in implementing an interoperable fingerprint identification system that can be used by the Departments of Justice, Homeland Security, State, and state and local law enforcement; and
- data integrity problems in the TSC database.

We originally planned to use evaluations we obtained from components to identify problems the Department has experienced in planning for IT systems. This was not possible because the Department has produced almost no meaningful evaluations of project management for either successful or failed IT projects, with the exception of two FBI projects. Post-implementation evaluations and audits of individual projects identified weaknesses in contract management, and excessive reliance on contractors.

Recommendations

We recommend that the CIO:

3. Ensure that post-implementation and post-termination evaluations are conducted that focus on lessons learned for project planning and management.
4. Ensure that staff receive training to obtain skills needed to adequately direct and oversee contractor efforts.
5. Implement targeted reviews to improve the use of business process re-engineering and requirements analysis early in concept development.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit, we considered management controls for the purpose of determining the Department's oversight role over IT studies, plans, and evaluations. This evaluation was not made for the purpose of providing assurance on the Department's internal controls for IT as a whole.

As described in the Findings and Recommendations section of this report, we identified weaknesses in the Department's oversight of IT studies, plans, and evaluations. We did not identify any additional weaknesses.

Because we are not expressing an opinion of the Department's internal controls over IT as a whole, this statement is intended solely for the information and use of the Department in managing its IT oversight role. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our audit objectives were to: (1) identify all research, plans, studies, and evaluations that the Department of Justice (Department) has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives; and (2) analyze the depth and scope of the problems the Department has experienced in the formulation of its IT plans.

Scope and Methodology

The audit was performed in accordance with the *Government Auditing Standards* and included tests and procedures necessary to accomplish the objectives.

This audit was performed in response to a congressional request included in the Department's appropriation for FY 2006. This report is the final in a series of three reports prepared by the OIG in response to the congressional request. Specifically, Congress instructed the OIG to present to the Committees on Appropriations: (1) an inventory of all major Department information technology (IT) systems and planned initiatives, and (2) a report that details all research, plans, studies, and evaluations that the Department has produced, or is in the process of producing, concerning IT systems, needs, plans, and initiatives. The report is also to include an analysis that will identify the depth and scope of problems the Department has experienced in the formulation of its IT plans. This report responds to the request for a report that details the research, studies, plans, and evaluations.

We identified relevant federal, Departmental, and component-specific requirements and standards for IT research, studies, plans, and evaluations, and merged the various standards into a generic set of documents.

We performed fieldwork at the:

Justice Management Division, Washington, D.C.;

Drug Enforcement Administration, Arlington, Virginia; and

Federal Bureau of Investigation, Washington, D.C.

We reviewed policy and procedures regarding processes related to capital planning and investment control, information technology investment management, and system development life-cycle processes.

We requested and obtained documents from the components to develop the inventory, and assessed compliance with the document standards for the major systems in the inventory. We did not limit the time period of documents we requested, because some of the systems and projects had been operational for many years and may have already prepared studies, plans, and evaluations.

To evaluate problems the Department has experienced in planning, we reviewed relevant audit and other independent reports, extending the scope of our audit work to some systems and projects that were not included in the inventory of major systems. We also analyzed the evaluations obtained for information about problems the Department has experienced in formulating IT plans.

APPENDIX II

ACRONYMS

Acronym	*Represents*
AFMS	Automated Facilities Management System
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
ATO	Approval to Operate
AU	Accreditation Unit
BOP	Bureau of Prisons
BPR	Business Process Reengineering
BRIDG	Biometric Reciprocal Identification Gateway
C&A	Certification and Accreditation
CAIR	Case Agent Image Review
CARA	Certification and Accreditation Reporting Application
CART	Computer Analysis Response Team
CARTSAN	Computer Analysis Response Team Storage Area Network
CASE	Computer Assisted Software Engineering
CDX	Counterdrug Intelligence Executive Secretariat
CITP	Classified Information Technology Program
CJIS	Criminal Justice Information Services
CM/CSA	Case Management/Common Solution Architecture
CMP	Configuration Management Plan
CODIS	Combined DNA Index System
COOP	Continuity of Operations Plan
CPOT	Consolidated Priority Organization Target
CSOS	Controlled Substances Ordering Systems
DCISS	DEA Classified Infrastructure Support System
DCS	Digital Collection System
DCU	Data Centers Unit
DEA	Drug Enforcement Administration
DEEP	Data Extraction and Extension Project
DERB	Department Executive Review Board
DHS	Department of Homeland Security
DIRB	Department Investment Review Board
DME	Develop, Modify, Enhance
EA	Enterprise Architecture
E-Com	Electronic Commerce
EDMS	ELSUR Data Management System
EIMO	ELSUR Information Management Office

Acronym	*Represents*
EIS	EPIC Information Systems
ELSUR	Electronic Surveillance
EOIR	Executive Office for Immigration Review
EOS	Enterprise Operations Services
EOUSA	Executive Offices for the United States Attorney
EPCS	Electronic Prescriptions for Controlled Substances
EPIC	El Paso Intelligence Center
ESOC	Enterprise Security Operations Center
ESS	EPIC Seizure System
EVENTS	Events Activity Subsystem
EVM	Earned Value Management System
FBI	Federal Bureau of Investigation
FCA	Facilities Certification and Accreditation
FDF-A	Financial Disclosure Forms Analyzer
FISMA	Federal Information Security Management Act
FITS	Infrastructure Technology Services
FMS	Fingerprint Matching Subsystem
FTTTF	Foreign Terrorist Tracking Task Force
GAN	Grant Adjustment Notice
IAFIS	Integrated Automated Fingerprint Identification System
IAS	Information Assurance Section
IATI	Information Assurance Technology Infusion
IBIS	Integrated Ballistics Information System
IDENT	DHS Automated Biometric Identification System
iDSM	interim Data Sharing Model
IDW	Investigative Data Warehouse
IMA	Investigative Mainframe Application
IMPACT	Investigative Management Program and Case Tracking System
IMPRB	Investment Management/Project Review Board
IODM	Input/Output Device Management
IPR	Intellectual Property Rights
IRIES	Immigration Review Information Exchange System
IRSS	Intelligence Research Support System
IT	Information Technology
ITCP	Information Technology Contingency Plan
ITD	Investigative Technologies Division
ITN	Identification Tasking and Networking
ITOD	Information Technology Operations Division
ITS-II	Inmate Telephone System II

Acronym	*Represents*
IWN	Integrated Wireless Network
JCON	Justice Consolidated Office Network
JCON-S	Justice Consolidated Office Network - Secret
JCON-TS	Justice Consolidated Office Network - Top Secret
JGMS	Justice Grants Management System
JMD	Justice Management Division
JPO	Joint Program Office
JSIT	Justice Secret Information Technology
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LCMS	Litigation Case Management System
LEO	Law Enforcement Online
LMIT	Lockheed Martin Integration Task
M204	Model 204 Corporate Systems
MADI	Manufacturers and Distributors
MDE	Managed Development Environment
NCIC	National Crime Information Center
N-DEx	Law Enforcement National Data Exchange
NDSS	National Drug Seizure System
NGI	Next Generation Identification
NIBIN	National Integrated Ballistics Information Network
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
OCDETF	Organized Crime Drug Enforcement Task Force
OCIO	Office of the Chief Information Officer
ODAG	Office of the Deputy Attorney General
OFC	OCDETF Fusion Center System
OJP	Office of Justice Programs
OMB	Office of Management and Budget
OTIS	Operational Test for Impact on Security
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PMO	Program Management Office
PMP	Project Management Plan
PMR	Program Management Review
POAM	Plans of Actions and Milestones
POC	Point of Contact
PTA	Privacy Threshold Analysis

Acronym	*Represents*
QAP	Quality Assurance Plan
RAMP	Risk Assessment and Management Plan
R-DEx	Regional Data Exchange
RITS	Request for Information Technology Services
RMP	Risk Management Plan
RTM	Requirements Traceability Matrix
SAE	Secret Administrative Enclave
SANS	Storage Area Networks
SCION	Secure Compartmented Information Operational Network
SDLC	System Development Life Cycle
SEMP	Systems Engineering Management Plan
SITP	System Integration and Test Plan
SMIS	Security Management Information System
SOW	Statement of Work
SPIU	Systems Programming & Integration Unit
SRTM	Security Requirements Traceability Matrix
SSAA	System Security Authorization Agreement
SSIAC	Security System Integration and Assessment Center
SSP	System Security Plan
TACLANE	Tactical Fastlane
TEMP	Test and Evaluation Master Plan
TI	Technology Infusion Program
TRP	Technology Refreshment Program
TRUFACS	Trust Fund Accounting and Commissary System
TS/SCI	Top Secret/Special Compartmented Information
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Center Database
UCR	Uniform Crime Reporting [Program]
UFMS	Unified Financial Management System
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
W2KE	Windows 2003
WBS	Work Breakdown Structure

Appendix III

IT STRATEGIC PLANS

Organization	*Document Title*	*Document Date*
DOJ	DOJ IT Strategic Plan, Fiscal Years 2006-2011	Jun 2006
ATF	Information Technology Strategic Plan, 2006-2011	
BOP	Information Technology Strategic Plan, FY 2004-2009	
DEA	IT Strategic Plan, FY 2005-2009	
EOIR	Strategic Plan, Information Resource Management, Fiscal Years 2005-2010	Feb 2006
FBI	Information Technology Strategic Plan, FY 2007-2011	Oct 2005

Source: Department of Justice components

Other studies, plans, and evaluations are listed in Appendix VI with the summary of each system or project.

APPENDIX IV

COMPLIANCE MATRIX[42]

Test Name	DEA Concorde	DEA E-Com	DEA EPIC	DEA Firebird	DEA M204	DEA Merlin
Market/Other Research			427, 432	1379		
Business Case Studies	*26, 32*	58, 61, 64	77*, 428, 430, 1401, 1403*	*123, 136*, 1378	80	271
Privacy Impact Assessment	35	56	1411			
Risk Management Plans	46, *47*	60, 72	417, 429, 1404, 1408		*1394*	261, *271*
Acquisition Plans	49		*1400*	*1380*		*271*
Project Plans	42, *48*	*70, 71,* 68	*419, 1402*, 1405	*128*, 129, *133, 135*	82, *1022*	*266,* 268
Security Plans	*25*, 50	74	420*, 421, 431, 1400*	*124, 140*, 1021	85	272
Systems Engineering Management Plans		65	424, *1400*			*1427, 1428, 1429*
Configuration Management Plans	*28*, 29	53	425, *1400*	116	81	1431
Quality Assurance Plans	83	67	83	130	83	83, 1432
Verification and Validation Plans		*75*	426		79	*1423, 1424, 1425, 1426*
Test Plans	44	52, 75	1409, 1412	131	1420	1384
Conversion Plans						
Implementation Plans	41	*65*		118, 139		*1430, 1433*

[42] The numbers in the columns refer to the document numbers in Appendix V. For example, the number 32 under Business Case Studies for DEA Concorde refers to Appendix V, item number 32, which is the Cost/Benefit Analysis Report for IMPACT, (a part of the Concorde project). Numbers shown in normal font are documents we are reporting as studies, plans, and evaluations, as opposed to other artifacts we accepted as contributing to compliance in each area, which are shown in italics. Shaded cells indicate that we obtained no documents or other artifacts that we accepted in response to our request.

Test Name	DEA Concorde	DEA E-Com	DEA EPIC	DEA Firebird	DEA M204	DEA Merlin
Training Plans	51	76	423			*1422*
Contingency/ COOP	30, *31*	54, 55	422	141		259
Disposition Plans						
Requirements Evaluations						
Test Evaluations	*23, 24*, 40, 50	73	1410, 1412	*131*, 137	1421	*257, 258*, 260, 272, 1385
Performance Evaluations	38			117, *120,* 121, 132, *138*		262, 264*, 265*
Post-implementation Evaluations		57		*117*		

Test Name	JMD CITP	JMD IWN	JMD JCON	JMD LCMS	JMD PKI	JMD UFMS
Market/Other Research	154	1388	227, 1012	250	232	*1417*, 1418, *1419*
Business Case Studies	*157*, 158, 173	198, *201*, 206, *1389*	*227, 228, 229*, 387	*248, 250*, 252, 256	216, *217, 232, 233*, 1017	*90, 91*, 99
Privacy Impact Assessment	161, 162, 175, 176		380, 390	1383	235	1399
Risk Management Plans	180, 181, 182	*204, 206*, 211	*387, 391, 392, 393, 394, 398, 399*, 400, *408*	*254*	*225, 231, 236, 239, 240*	*99*, 101, *110*
Acquisition Plans	142, *159, 173*	195, *206*	374, *387, 391, 392, 393, 394*			86, 87, *99*
Project Plans	*155*, 171, 177, *179*	*205*, 209, 1004	*387*, 391, 392, 393, 394, 1005	254, *255*	236, *1008*	93, 94
Security Plans	*183*, 188, 189	*199, 206*, 214	*387, 391, 392, 393, 394,* 404		*231*, 244	*100*, 103, 105
Systems Engineering Management Plans	*152*	*205*	407			96
Configuration Management Plans	146, 147	196	372	253	*219*, 220	88, 89
Quality Assurance Plans		210	*376, 377, 378, 379, 382, 388, 395*	*254*	*230, 236*	95
Verification and Validation Plans	153, *190*	192, 193, 194	*384*			
Test Plans	*153*, 168, *184, 185*, 186	192, 193, 194, 213	405, 406		245	97
Conversion Plans	150		*379, 382*			92
Implementation Plans	151*, 187*	203, 215	379, 382		222	106
Training Plans	145	208	*379, 382*		247	109
Contingency/ COOP	148, 149	197	373		226	
Disposition Plans					218	
Requirements Evaluations						
Test Evaluations	*143, 160*, 168, 186	*212*	401, 403		*231*, 242, 246	

Test Name	JMD CITP	JMD IWN	JMD JCON	JMD LCMS	JMD PKI	JMD UFMS
Performance Evaluations		202	375		*221*, 223, *243*	*99*
Post-implementation Evaluations		202	371, 385, 386, 402		*238*	

Test Name	ATF NIBIN	BOP ITS-II	EOIR e-World	ODAG OFC	OJP JGMS
Market/Other Research	*7, 8*	416	854	1369, *1370*, 1371, 1372, *1374, 1375, 1376,* 1377	
Business Case Studies	8	18, 1392	*111,* 112	*276, 292, 294, 304,* 316, *327*	*345, 349, 360*, 364
Privacy Impact Assessment	9	20	860	320	
Risk Management Plans	*7, 8, 13*	*412, 413*	*112, 114, 115*	*316, 318, 326,* 328, *330, 331*	*360, 364, 368*
Acquisition Plans	*8*, 12	19	*112*	*274, 275*, 306	*364*
Project Plans		412	851, 852, *853*	321, 322, *323, 1013, 1014*	*352, 353*, 360
Security Plans	14	21	*113*, 863, *865, 867*	334	340
Systems Engineering Management Plans		415			
Configuration Management Plans			856, 857		341, *363*
Quality Assurance Plans			*868*	83, *321*	
Verification and Validation Plans					*346, 347, 348, 350, 351, 357, 360*
Test Plans	15, 1397, 1398		*864*	*284, 288, 303, 324, 325*, 335	346, 347, 348
Conversion Plans		22			
Implementation Plans	1413, 1414, *1415, 1416*	22	*851, 852, 853*	*287*	*352, 353, 356, 360*
Training Plans	17			289	359
Contingency/ COOP	2, 3	414	855	305	342
Disposition Plans					
Requirements Evaluations					
Test Evaluations	15, 16, 1395, 1396	*409*	*864*	*278, 279, 281, 282, 290, 297, 335, 336*, 338	345*, 350, 351*, 357, *366*, 1390

Test Name	ATF NIBIN	BOP ITS-II	EOIR e-World	ODAG OFC	OJP JGMS
Performance Evaluations	*7, 8, 11*		*862*	*277, 298, 300, 301, 308, 309, 310, 313, 314*	*343, 344, 354, 355, 358, 364*
Post-implementation Evaluations				*311*	

Test Name	FBI BRIDG	FBI CARTSAN	FBI CODIS	FBI DCS	FBI DCU	FBI EDMS	FBI FTTTF
Market/Other Research							
Business Case Studies	454, *455, 457*, 1036	*437, 444*, 1023	*465*, 467, *468, 469*	*493, 494, 495, 523*, 1024	*486*, 489	*540, 542, 550, 552*, 1025	*558, 559, 562, 563*, 1026
Privacy Impact Assessment	459	446	471	510, 511		529	
Risk Management Plans	*458*, 462	447, *448*	473, *474*	521	*478, 487, 488, 489*	547, 548, *549*	565, *566*
Acquisition Plans			475				
Project Plans	*456*	*450*	*466*, 472	498, *501*, 516, 517, 518, 519, *528*	481, *487, 488, 489,* 490	544, *545*	564
Security Plans		*435*, 449	*464, 470*, 476,	*497, 499, 500, 522*, 524, 525, 526	*479, 489*, 492	*530*, 553	
Systems Engineering Management Plans							567
Configuration Management Plans		438		*496*		532	
Quality Assurance Plans		439					
Verification and Validation Plans							
Test Plans		436		527	*485*	531, 555	*560, 568, 569, 570*, 571
Conversion Plans						554	
Implementation Plans		434				*537*	561
Training Plans		*442*				*551*	
Contingency/ COOP			477		480	533	
Disposition Plans					*484*		
Requirements Evaluations							
Test Evaluations		*436*					

Test Name	FBI BRIDG	FBI CARTSAN	FBI CODIS	FBI DCS	FBI DCU	FBI EDMS	FBI FTTTF
Performance Evaluations	*460, 461*	441, 443	*463*	509, 520	*483, 484, 487, 488, 489*, 491	535, 536, *538*, 543, 546	
Post-implementation Evaluations				514			

Test Name	FBI IAFIS	FBI IATI	FBI IDW	FBI LEO	FBI NCIC	FBI N-DEx
Market/Other Research						
Business Case Studies	1027	*600, 601, 605, 611*, 612		1017	*668, 674,* 1028	*695, 697*, 1029
Privacy Impact Assessment		613				1386
Risk Management Plans		616*, 617, 618*	631*, 632*	*656*	*683*, 684	700, *701*
Acquisition Plans						
Project Plans		*598, 609*, 614		*646,* 653	*679, 680*, 682	699, *1387*
Security Plans	588, 591	619, 623, 624	633	642	*685*, 688	702
Systems Engineering Management Plans	592, 593	621			687	
Configuration Management Plans	582	602		647	669	
Quality Assurance Plans	589	615				
Verification and Validation Plans	586					
Test Plans	577, 584	625, 626, 627		*637, 638, 639, 655*, 657	675, 676, 686, 690	694
Conversion Plans	596, 597	629	636	659	691, 693	
Implementation Plans	574, 576, 579, 580, 583	608, 622	*630*	643, 644, *649, 650, 651, 652*	670	
Training Plans	587, 595	628	635		681	
Contingency/ COOP				645		
Disposition Plans						
Requirements Evaluations						
Test Evaluations	573, 575, 578, 581, 585		634		665, 672, 673, 677, 678	
Performance Evaluations	*594*	*599, 604, 610*		*640, 641, 658*		

Test Name	FBI IAFIS	FBI IATI	FBI IDW	FBI LEO	FBI NCIC	FBI N-DEx
Post-implementation Evaluations	*594*	*606*			*689*	

Test Name	FBI NGI	FBI NICS	FBI R-DEx	FBI SCION	FBI Sentinel	FBI SMIS	FBI TRP	FBI TSC
Market/Other Research								
Business Case Studies	*703, 704, 705, 706, 707, 708, 714, 716*, 1030	*731*, 1031	1032		*766, 775*, 1033	*784, 788*, 797, *819, 820, 825*	*835, 836*, 1034	*849*, 1035
Privacy Impact Assessment	719, 720, 721, 722			751	1434	791, 792, 798		
Risk Management Plans	*728*, 729		662		*769*, 772	*816*, 817, *818, 832*		*840*, 845
Acquisition Plans					755, *773*, 1037, *1038*			
Project Plans	*715*, 726				*757, 759, 761*, 770	812, 813, 814, *823*		*844*, 849
Security Plans		*744*, 746	*663*, 664	753		826, 827		*839*, 846
Systems Engineering Management Plans					776			
Configuration Management Plans	709	732		752	758	785		
Quality Assurance Plans	727	743			771	815		
Verification and Validation Plans								848
Test Plans		730, 737, 747	660		777	782, 829, 831		*842*, 847, 848
Conversion Plans		742, 749						
Implementation Plans		740, 741, 745, 750						*838*
Training Plans						833		
Contingency/ COOP		733, 735						
Disposition Plans								
Requirements Evaluations								
Test Evaluations		739, *748*	661	754		*778*, 783, 828, *830*		843

Test Name	FBI NGI	FBI NICS	FBI R-DEx	FBI SCION	FBI Sentinel	FBI SMIS	FBI TRP	FBI TSC
Performance Evaluations	*710, 711*, 713, 725				*760, 762, 763, 764, 765,* 1039	786, 793, 794*, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811*	836	*850*
Post-implementation Evaluations								

APPENDIX V

DOCUMENTS AND OTHER ARTIFACTS[43]

Item ID Number	Component	System or Project	Title	Date
2	ATF	NIBIN	Contingency Plan - Appendix I, NIBIN	
3	ATF	NIBIN	Contingency Plan, NIBIN and IBIS	Jun 2005
7	ATF	NIBIN	OMB Exhibit 300 for BY 2005	Feb 2004
8	ATF	NIBIN	OMB Exhibit 300 for BY 2007	May 2006
9	ATF	NIBIN	Privacy Threshold Analysis, IBIS	
11	ATF	NIBIN	Project Management Review, NIBIN, Undated	
12	ATF	NIBIN	Request for Justification for Other Than Full and Open Competition	Jan 2002
13	ATF	NIBIN	Risk Assessment, NIBIN and IBIS	Jun 2005
14	ATF	NIBIN	Security Plan, NIBIN and IBIS	Jun 2005
15	ATF	NIBIN	Security Test and Evaluation, NIBIN	Dec 2005
16	ATF	NIBIN	Security Testing and Evaluation, NIBIN	Dec 2005
17	ATF	NIBIN	NIBIN Training Set 11, Version 1.2, Draft	
18	BOP	ITS-II	Analysis of Alternatives, Next Generation Inmate Telephone System	Jul 1996
19	BOP	ITS-II	Individual Acquisition Planning	Jan 1997
20	BOP	ITS-II	Privacy Impact Assessment	Apr 2006
21	BOP	ITS-II	Inmate Telephone System (ITS-II) Security Plan	Dec 2004
22	BOP	ITS-II	Site Network Integration Plan, ITS-II/TRUFACS	Nov 2001
23	DEA	Concorde	Accreditation Statement for Inclusion into Web Architecture IMPACT	Jul 2002
24	DEA	Concorde	Accreditation Statement, Office of Information Systems, Web Infrastructure	Oct 2004
25	DEA	Concorde	Action Plan, Independent Evaluation Pursuant to the FISMA FY 2004, DEA IMPACT System	
26	DEA	Concorde	Business Modeling Specification, IMPACT, BPR Task Order #1, Version 1.0	Sep 2004
28	DEA	Concorde	Configuration Management Plan, Concorde QA Findings Report	Oct 2004

[43] Documents and other artifacts are listed by document number assigned by auditors. This Appendix should be used with Appendix IV. This listing includes many acronyms associated with the systems and projects, but which were not used in the report. We included acronyms in the list in Appendix II for reference. Blank cells in the Date column indicate items for which no date was provided.

Item ID Number	Component	System or Project	Title	Date
29	DEA	Concorde	Configuration Management Plan, Concorde, Version 1.0	Jul 2004
30	DEA	Concorde	Contingency Plan, Web Architecture, Version 2.0	Mar 2006
31	DEA	Concorde	Contingency Plan, Web Architecture, Version 2.0 (Signature Pages)	Mar 2006
32	DEA	Concorde	Cost/Benefit Analysis Report, IMPACT, BPR Final Version	Apr 2000
35	DEA	Concorde	Initial Privacy Impact Assessment , Concorde	
38	DEA	Concorde	OCIO: Project Dashboard Project Managers Worksheet, Concorde	Aug 2005
39	DEA	Concorde	OMB Exhibit 300 for BY 2007	Sep 2005
40	DEA	Concorde	Operational Test for Impact on Security (OTIS) Report of the Pilot Implementation, IMPACT	Jul 2002
41	DEA	Concorde	Project Deployment Plan, Concorde, Version 1.0	Sep 2004
42	DEA	Concorde	Project Management (PMP), IMPACT Fiscal Year 2004, Version 2.1	Sep 2004
44	DEA	Concorde	Project Test Plan (PTP), IMPACT, Release 2.0, Version 1.0	Feb 2005
46	DEA	Concorde	Risk Management Plan, Concorde, Version 1.0	Feb 2005
47	DEA	Concorde	Risk Inventory & Assessment, Section I.F., OMB Exhibit 300	Mar 2005
48	DEA	Concorde	Original Baseline, Section I.H.2, OMB Exhibit 300	
49	DEA	Concorde	Statement of Work/Acquisition Plan, Concorde, Version 1.0	Nov 2002
50	DEA	Concorde	System Security Authorization Agreement (SSAA), Appendix E, Web Architecture	Mar 2002
51	DEA	Concorde	Training Program, PMP Concorde, FY 2006, Version 1.0	Oct 2005
52	DEA	E-Com	Acceptance Test Plan, Public Key Infrastructure Analysis, Diversion PKI, CSOS	Jan 2005
53	DEA	E-Com	Configuration Management Plan, DEA Diversion Control E-Commerce System, Version 1.0	Feb 2006
54	DEA	E-Com	Contingency Plan, DEA Diversion Control E-Commerce PKI System (EPCS/CSOS), Version 1.0	Nov 2003
55	DEA	E-Com	Contingency Plan, DEA Diversion E-Commerce System Security Plan, Appendix L, Version 1.1	May 2005
56	DEA	E-Com	Detailed Privacy Impact Assessment, Attachment: DEA CSOS Privacy Policy, Section IV	Sep 2005
57	DEA	E-Com	Diversion Metrics Implementation Report, DEA Diversion Control, E-Commerce System, Version 1.0	Jan 2006

Item ID Number	Component	System or Project	Title	Date
58	DEA	E-Com	Economic Impact Analysis of the Electronic Orders Rule	Mar 2005
60	DEA	E-Com	Facilitated Risk Assessment Process, DEA Diversion Control E-Commerce PKI, SSAA, Appendix G, Version 1.0	Dec 2003
61	DEA	E-Com	Initial Economic Impact Analysis of the Proposed Electronic Orders Rule	Mar 2005
64	DEA	E-Com	OMB Exhibit 300 for BY 2007, Final CSOS	Sep 2005
65	DEA	E-Com	Operational and Technical Architecture, Public Key Infrastructure Analysis, DEA Diversion Control E-Commerce PKI	Jun 2003
67	DEA	E-Com	Process and Product Quality Assurance, DEA Diversion Control E-Commerce System, Version 1.0	May 2005
68	DEA	E-Com	Program Management Plan, DEA Diversion Control E-Commerce PKI, Version 3.1	Nov 2004
70	DEA	E-Com	Project Plans, CSOS FY05, Undated	
71	DEA	E-Com	Project Plans, CSOS FY06, Undated	
72	DEA	E-Com	Risk Management Plan, DEA Diversion Control, E-Commerce System, Version 1.0	Oct 2005
73	DEA	E-Com	System Security Authorization Agreement (SSAA), Appendix F, CSOS and EPCS PKI	Mar 2004
74	DEA	E-Com	System Security Plan, CSOS, Version 1.0	Jun 2005
75	DEA	E-Com	Test Plan and Reporting Procedures, CSOS/ EPCS	Dec 2001
76	DEA	E-Com	Training Plan, Public Key Infrastructure Analysis, DEA Diversion Control E-Commerce PKI	Aug 2002
77	DEA	EPIC	OMB Exhibit 300 for BY 2007	Sep 2005
79	DEA	M204	Independent Verification and Validation (IV&V) Software Testing Procedure for Mainframe Environment, Version 2.0	Jun 2004
80	DEA	M204	OMB Exhibit 300 for BY 2007	Jul 2005
81	DEA	M204	Project Level Configuration Management Plan, Events Activity Subsystem (EVENTS), Version 1.0	Jun 2004
82	DEA	M204	Project Management Plan (PMP), Events Activity Subsystem (EVENTS), Calendar Year 2004, Version 1.0	Jun 2004
83	DEA	Concorde	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005
83	DEA	EPIC	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005
83	DEA	M204	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005

Item ID Number	Component	System or Project	Title	Date
83	DEA	Merlin	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005
83	ODAG	OFC	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005
85	DEA	M204	Systems Security Authorization Agreement (SSAA), Model 204 Corporate Systems	Nov 2004
86	JMD	UFMS	Acquisition Plan UFMS Integration and Implementation Services, (Draft)	Jun 2005
87	JMD	UFMS	Acquisition Strategy Paper, DOJ UFMS	Jun 2002
88	JMD	UFMS	Configuration Management Plan, Version 1.0	Aug 2005
89	JMD	UFMS	Configuration Management Plan, Version 2.0	Jun 2006
90	JMD	UFMS	Cost Benefit Analysis, DOJ UFMS Project	May 2003
91	JMD	UFMS	Cost Benefit Analysis, Draft	Mar 2004
92	JMD	UFMS	Data Conversion Strategy, Version 1.0	Jul 2006
93	JMD	UFMS	DOJ Program Office Charter and Program Management Plan, Version 2.0	Sep 2004
94	JMD	UFMS	Implementation and Integration - Project Management Plan, Version 1.0	Jun 2006
95	JMD	UFMS	Integration and Implementation - Quality Control Plan, Version 1.0	Jul 2006
96	JMD	UFMS	Integration and Implementation - Systems Engineering Plan	Jul 2006
97	JMD	UFMS	Integration and Implementation Test and Evaluation Master Plan	Jul 2006
99	JMD	UFMS	OMB Exhibit 300 for BY 2007	Dec 2005
100	JMD	UFMS	POAM Report, UFMS	Dec 2005
101	JMD	UFMS	Risk and Issue Management Plan, Version 2.0	Sep 2004
103	JMD	UFMS	Security Management Plan (UFMS), Version 1.0	Jan 2006
105	JMD	UFMS	System Security Plan (SSP) for DOJ UFMS	Dec 2005
106	JMD	UFMS	System Implementation Plan, Version 1.0	Jul 2006
109	JMD	UFMS	Training Strategy, Version 1.0	Jul 2006
110	JMD	UFMS	Vulnerability/ Countermeasures and Threat Pairing, UFMS	Dec 2005
111	EOIR	eWorld	Alternatives/Cost Benefit Analysis Report for Alternatives Analysis of eWorld for FY 2005	Mar 2005
112	EOIR	eWorld	OMB Exhibit 300 for BY 2007	Jan 2006
113	EOIR	eWorld	Residual Risk Report for JCON-II/CASE, EOIR	Nov 2005
114	EOIR	eWorld	Risk Management and Areas of Concern	Mar 2006
115	EOIR	eWorld	Vulnerability/Countermeasures and Threat Pairing	Mar 2006
116	DEA	Firebird	Configuration Management Plan (CMP), FITS, Version 1.3	Jan 2006

Item ID Number	Component	System or Project	Title	Date
117	DEA	Firebird	Enterprise Health and Performance Metrics Review	May 2006
118	DEA	Firebird	EOS Software Deployment Function Description, Version 2.5, not dated	
120	DEA	Firebird	Firebird Daily Status Report	Jul 2006
121	DEA	Firebird	Firebird Dashboard	Apr 2006
123	DEA	Firebird	Firebird Extension and Growth Strategy	Mar 1995
124	DEA	Firebird	Firebird Security Overview	Jun 2006
128	DEA	Firebird	Program Management Plan, Firebird Documentation EOS, Version 1.0 (Draft)	
129	DEA	Firebird	Project Management Plan (PMP), Firebird Infrastructure Technology Services (FITS), Version 3.0	Jan 2006
130	DEA	Firebird	Quality Assurance Plan, FITS, Version 2.1	Jan 2005
131	DEA	Firebird	Security Test and Evaluation Plan and Procedures, Appendix E	Jul 2004
132	DEA	Firebird	SIO Firebird project portfolio	Jul 2006
133	DEA	Firebird	SIOM Firebird Sensitive but Unclassified (SBU) Infrastructure O&M Strategic Goals & Tactical Plan	
135	DEA	Firebird	Statement of Work for Enterprise Wide Management	Sep 2000
136	DEA	Firebird	Storage Matrix/SRA	
137	DEA	Firebird	Test Matrix, Desktop and Server Management Evaluation 2005	
138	DEA	Firebird	Weekly Status Report, Enterprise Operations Services	Jun 2006
139	DEA	Firebird	Windows 2003 (W2K3) Implementation Plan, FITS MDE, Version 1.2	Jun 2006
140	DEA	Firebird	Windows 2003 Active Directory Security Groups and Group Policy, FITS, Version 1.4	Jun 2006
141	DEA	Firebird	Windows Server 2003 Infrastructure Disaster Recovery Document, FITS, Version 2.1	Jun 2006
142	JMD	CITP	Acquisition Plan, CITP, Version 1.0	Jan 2006
143	JMD	CITP	Test Cases for the Enterprise Security Operations Center (ESOC)	Sep 2004
145	JMD	CITP	Computer Security Awareness and Training (C/SAT) Plan, JCON-S Enterprise System, Version 2.1	Dec 2003
146	JMD	CITP	Published Documents, Configuration Management Plan, JCON-S, Version 1.0	May 2004
147	JMD	CITP	Configuration Management Process, JCON-S, Appendix V, Version 1.1	Dec 2003
148	JMD	CITP	Contingency Plan, JWICS Network, Appendix M	
149	JMD	CITP	Contingency Plan, JCON-S, Appendix L	Feb 2004
150	JMD	CITP	Data Migration, ADNET to JCON-S	
151	JMD	CITP	Sample JSIT Deployment Plan	

Item ID Number	Component	System or Project	Title	Date
152	JMD	CITP	Design Methodology, CITP	
153	JMD	CITP	Engagement Security Approach, JCON-S	
154	JMD	CITP	Enterprise Proof-of-Concept Functional Requirements, JSIT, Version 1.1	Dec 2003
155	JMD	CITP	Enterprise Proof-of-Concept Project Schedule	
157	JMD	CITP	Final Classified Networks Program E-Survey Findings	Jun 2003
158	JMD	CITP	Fiscal Year 2005 Information Technology Concept Paper	
159	JMD	CITP	Hardware and Software Vendor Maintenance, JCON-S, (Draft)	Feb 2004
160	JMD	CITP	Host Vulnerability Summary Report, Appendix G	Oct 2003
161	JMD	CITP	Initial Privacy Impact Assessment, JCON-S	
162	JMD	CITP	Initial Privacy Impact Assessment, JCON-TS	
168	JMD	CITP	Acceptance Test Plan and Report	Dec 2003
171	JMD	CITP	MOA between JCON and DTO Regarding Operation and Support of the JCON Classified Infrastructure, Version 0.2, Draft	Dec 2003
173	JMD	CITP	OMB Exhibit 300 for BY 2006	
175	JMD	CITP	Privacy Threshold Analysis, JCON-S	
176	JMD	CITP	Privacy Threshold Analysis, JCON-TS	
177	JMD	CITP	Program Guide, JCON-S, Version 2.1	May 2005
179	JMD	CITP	Project Schedule	
180	JMD	CITP	Risk Assessment/Risk Matrix, JWICS	Dec 2003
181	JMD	CITP	Risk Management Plan, Enterprise SIPRNET, Draft	Mar 2003
182	JMD	CITP	Risk Management Plan, JIST, Version 1.0, Draft	Jul 2006
183	JMD	CITP	Security Requirements Extract, JCON-TS	
184	JMD	CITP	Security Requirements Traceability Matrix, JWICS Network, Appendix F, Software Version, 1.0.0.2	Dec 2003
185	JMD	CITP	Security Requirements/Security Requirements Traceability Matrix, JCON-S, Appendix D	Feb 2004
186	JMD	CITP	Security Test and Evaluation Plan, JCON-S, Appendix E	Feb 2004
187	JMD	CITP	Standard Deployment Process (Chart)	
188	JMD	CITP	System Security Authorization Agreement (SSAA), JCON-S	Feb 2004
189	JMD	CITP	System Security Plan, JWICS Network, JCON-TS	Dec 2003
190	JMD	CITP	Task Outline for Security Scans of JCON-S and JCON-TS	Mar 2004
192	JMD	IWN	Data System Functional Tests, JPO-Pilot System	Oct 2004
193	JMD	IWN	Network Management	Oct 2004
194	JMD	IWN	Report Generation Tests	Oct 2004
195	JMD	IWN	Acquisition Plan, IWN JPO	Aug 2004

Item ID Number	Component	System or Project	Title	Date
196	JMD	IWN	Configuration Management Plan, JPO IWN	Jun 2004
197	JMD	IWN	Contingency Plan, JPO IWN Northwest Zone	Jun 2005
198	JMD	IWN	High Level Design Report	
199	JMD	IWN	Incident Response Plan, Seattle-Blaine Beta Test System	Sep 2004
201	JMD	IWN	Requirements Document, IWN, (Working Draft)	Jun 2002
202	JMD	IWN	Beta Benchmark Assessment, IWN Seattle/Blaine	
203	JMD	IWN	Organizational Readiness Transition Activities, IWN Seattle-Blaine Service Area	Sep 2004
204	JMD	IWN	Risk Assessment, IWN BETA Test System	Sep 2004
205	JMD	IWN	Master Beta Schedule, JPO	Jul 2003
206	JMD	IWN	OMB Exhibit 300 for BY 2007	Jan 2006
208	JMD	IWN	Personnel Training for the Integrated Wireless Network	Nov 2004
209	JMD	IWN	Program Plan FY 2006, Joint Program Office, Draft	Jun 2005
210	JMD	IWN	Quality Assurance Plan, DOJ Wireless Network	
211	JMD	IWN	Risk Management Plan, DOJ Wireless Management Office, Justice Wireless Network	Jun 2006
212	JMD	IWN	Seattle-Blaine System Acceptance Tests on CD	
213	JMD	IWN	Security Test and Evaluation Report: Beta Test System	Nov 2004
214	JMD	IWN	System Security Plan, Beta Test System	Nov 2004
215	JMD	IWN	Transition Plan	Oct 2004
216	JMD	PKI	Business Case, DOJ Enterprise PKI, Version 1.0	Jul 2004
217	JMD	PKI	Business Case, Insource vs. Outsource, DOJ Enterprise PKI	Apr 2006
218	JMD	PKI	Chain of Custody Processes, DOJ PKI, Version 1.01	Jun 2005
219	JMD	PKI	Configuration Guide, DOJ PKI, Draft	Mar 2005
220	JMD	PKI	Configuration Management Plan, DOJ PKI Program and Technical Support, Version 1.1, Draft	Mar 2005
221	JMD	PKI	Department Executive Review Board Presentation	Oct 2005
222	JMD	PKI	Deployment Implementation Plan, DOJ PKI, Final	Jun 2005
223	JMD	PKI	Earned Value Management, DOJ Enterprise PKI Infrastructure Service Office	
225	JMD	PKI	Risk Review HSPD-12, DOJ Enterprise System Solution, Infrastructure Services Office	
226	JMD	PKI	IT Contingency Plan, DOJ PKI, Appendix L, Revision 3	Mar 2006
227	JMD	JCON	JCON Architecture Study, Final Report	Jan 1998
228	JMD	JCON	JCON Shared Services Model	
229	JMD	JCON	JCON Strategic Plan: Arguments/Counter Arguments	Aug 2005
230	JMD	PKI	Phase 2 Task Order, DOJ Enterprise PKI	May 2004
231	JMD	PKI	Plan of Actions and Milestones (POAM)	Jul 2006

Item ID Number	Component	System or Project	Title	Date
232	JMD	PKI	Planning and Design Support, DOJ PKI	Oct 2002
233	JMD	PKI	Position Paper for JUTnet RAS PKI Support	Oct 2005
235	JMD	PKI	Privacy Threshold Analysis (questionnaire)	
236	JMD	PKI	Project Management Plan, DOJ PKI	Aug 2004
238	JMD	PKI	Results of survey, Criminal Division, PKI Pilot	
239	JMD	PKI	PKI Risk Registry	Apr 2006
240	JMD	PKI	Risk Management Overview, DOJ Enterprise System Solution, Infrastructure Services Office	
242	JMD	PKI	Security Test and Evaluation Plan (Final), DOJ PKI	May 2005
243	JMD	PKI	Status Report, DOJ PKI	Jun 2006
244	JMD	PKI	System Security Plan, DOJ PKI, Revision 2	Mar 2006
245	JMD	PKI	Test and Evaluation Master Plan, DOJ PKI, Revision 1	Apr 2005
246	JMD	PKI	Test Report, DOJ PKI, Draft	Jun 2005
247	JMD	PKI	Training Plan, DOJ PKI, Final	Apr 2005
248	JMD	LCMS	Business Concept of Operations, LCMS, Version 1.1	Oct 2005
250	JMD	LCMS	Final Market Research Report, LCMS	Jun 2005
252	JMD	LCMS	OMB Exhibit 300 for BY 2007	Dec 2005
253	JMD	LCMS	Project Configuration Management Plan, Version 1.1	Apr 2005
254	JMD	LCMS	Project Management Plan, Version 1.2	Aug 2005
255	JMD	LCMS	Project Plan, LCMS (Spreadsheet)	Apr 2006
256	JMD	LCMS	Technical Evaluation Report, LCMS Phase 1, Version 0.9, Final	Apr 2006
257	DEA	Merlin	Accreditation Approval DCISS	Jan 2004
258	DEA	Merlin	Approval Request for Accreditation DCISS	Aug 2003
259	DEA	Merlin	Contingency Plan for the DEA Merlin Program	Jun 2006
260	DEA	Merlin	COOP Test Report using VERITAS Replication EXEC 3.1	Mar 2006
261	DEA	Merlin	Risk Assessment Report, DEA Classified Infrastructure Support System	May 2005
262	DEA	Merlin	Earned Value Management (EVM) Merlin, Doc #12-35-41-55	Jul 2006
264	DEA	Merlin	Merlin Dashboard - May	Jun 2006
265	DEA	Merlin	Merlin Engineering Review	Apr 2006
266	DEA	Merlin	Merlin WBS/Schedule	Mar 2006
268	DEA	Merlin	Merlin Program Plan, Version 2	Jun 2006
271	DEA	Merlin	OMB Exhibit 300 for BY 2007	
272	DEA	Merlin	System Security Authorization Agreement (SSAA), DCISS	Aug 2003
274	ODAG	OFC	Acquisition Strategy for BY 2007	
275	ODAG	OFC	Acquisition Strategy	
276	ODAG	OFC	Alternative Analysis	

Item ID Number	Component	System or Project	Title	Date
277	ODAG	OFC	ANSI 748 Compliance Plan	Aug 2005
278	ODAG	OFC	Assessment of Defects on Hold (Spreadsheet)	
279	ODAG	OFC	Beta Testing Start Criteria and Status, OFC Compass (Spreadsheet)	Apr 2006
281	ODAG	OFC	Compass Defect Summary Report	Jun 2006
282	ODAG	OFC	Compass Defect Summary Report (Spreadsheet)	Jun 2006
284	ODAG	OFC	Compass Functional Testing Work Plan (Spreadsheet)	Jan 2006
287	ODAG	OFC	Compass System "Go-Live" Timeline	
288	ODAG	OFC	Compass Testing Timeline	
289	ODAG	OFC	Compass Training Plan, OFC, Version 1.0	Sep 2005
290	ODAG	OFC	Compass User Acceptance Test Summary Status	May 2006
292	ODAG	OFC	Concept of Operations, OCDETF Fusion Center	Mar 2004
294	ODAG	OFC	Cost Benefit Analysis, OFC System	Dec 2004
297	ODAG	OFC	Defect Recommendations (Spreadsheet)	
298	ODAG	OFC	Dept Executive Review Board Presentation, OFC	Nov 2005
300	ODAG	OFC	Direct Funding for the Development of the OFC (Spreadsheet)	
301	ODAG	OFC	DOJ/OCIO Executive Review, OFC	Jan 2005
303	ODAG	OFC	Functional Testing Process Flow	
304	ODAG	OFC	Fusion Center Overview and Drug Intelligence Analysis Report, Drug Intelligence Fusion Center	
305	ODAG	OFC	IT Contingency Plan, IRSS, Version 2.2	Mar 2005
306	ODAG	OFC	Justification for Other than Full and Open Competition	May 2004
308	ODAG	OFC	List of Milestones and Deliverables	Oct 2005
309	ODAG	OFC	OCDETF Fusion Center EVM Report (Spreadsheet)	Mar 2006
310	ODAG	OFC	OCDETF Fusion Center Review Meeting Agenda	Jun 2006
311	ODAG	OFC	OFC Compass Release 1.0 Capability Assessment	Apr 2006
313	ODAG	OFC	OFC Master Schedule – No Ops – Merrifield (Spreadsheets)	
314	ODAG	OFC	OFC Master Schedule – No Ops – NS IOC (Spreadsheets)	
316	ODAG	OFC	OMB Exhibit 300 for BY 2006	Sep 2004
318	ODAG	OFC	OMB Exhibit 300 for BY 2007	
320	ODAG	OFC	Privacy Impact Assessment, OFC (Draft)	Aug 2004
321	ODAG	OFC	Project Management Plan, OFC Deployment	Sep 2005
322	ODAG	OFC	Project Plan, Software Version 1.0, OFC	May 2006
323	ODAG	OFC	Project Schedule, WBS CCB CR41(Spreadsheets)	
324	ODAG	OFC	Requirements Traceability Table	Jan 2006
325	ODAG	OFC	Requirements Traceability Table, Script Case Mapping to Requirements	Jan 2006
326	ODAG	OFC	Residual Risk Report, OFC	May 2006

Item ID Number	Component	System or Project	Title	Date
327	ODAG	OFC	Risk Adjusted Cost Formulation	
328	ODAG	OFC	Risk and Issue Management Master Plan	Jun 2005
330	ODAG	OFC	Risk Assessment Results for BY 2006	
331	ODAG	OFC	Risk Assessment Results for BY 2007	
334	ODAG	OFC	System Security Plan, OFC Compass	
335	ODAG	OFC	System Test Plan, OFC, Version 1.2	Jan 2006
336	ODAG	OFC	Testing Status Summary	Sep 2006
338	ODAG	OFC	Validation Test Script Forms	May 2006
340	OJP	JGMS	System Security Plan for Grants Management System	Feb 2006
341	OJP	JGMS	Configuration Management Plan, OJP	Nov 2004
342	OJP	JGMS	Continuity of Operations Plan, OJP	Jul 2005
343	OJP	JGMS	Detailed Design Review GMS/Grant Adjustments	Jan 2006
344	OJP	JGMS	Detailed Design Review GMS/Grant Adjustments, Phase 1, Installment 2	Jan 2006
345	OJP	JGMS	Functional Requirements Document, Grant Adjustments, OJP, Version 1.1	Nov 2005
346	OJP	JGMS	GMS Grant Adjustment Notice Module Test Cases	Oct 2005
347	OJP	JGMS	GAN Module Test Plan, OJP	
348	OJP	JGMS	Grant Adjustment Notice Module Test Plan, Phase 2	
349	OJP	JGMS	GAN Module, Software Requirements Specification Use Cases, Draft, Version 1.5	May 2006
350	OJP	JGMS	GAN Phase 1 – STR	Mar 2006
351	OJP	JGMS	GAN Phase 2 – STR	May 2006
352	OJP	JGMS	GAN Schedule	Sep 2005
353	OJP	JGMS	GAN Schedule	Dec 2005
354	OJP	JGMS	GAN Schedule – EVM	Apr 2006
355	OJP	JGMS	GAN Schedule – EVM	Feb 2006
356	OJP	JGMS	GAN Schedule – EVM	May 2006
357	OJP	JGMS	GAN Test Problem Report (Spreadsheet)	
358	OJP	JGMS	GMS EVM (Spreadsheet)	Apr 2006
359	OJP	JGMS	GMS GAN Training Plan, (Draft)	May 2005
360	OJP	JGMS	Grant Adjustment Notice (GAN) Module Project Management Plan, Draft	Sep 2005
363	OJP	JGMS	OJP Change Control Procedures, Version 2.0	Feb 2006
364	OJP	JGMS	OMB Exhibit 300 for BY 2007	
366	OJP	JGMS	Preliminary Design Review GMS/GAN Module	Oct 2005
368	OJP	JGMS	Risk Management Plan, Version 1.1 (Spreadsheet), GAN	Oct 2006
371	JMD	JCON	Civil Rights Division Lessons Learned Report, JCON IIA Implementation Phase	May 2006

Item ID Number	Component	System or Project	Title	Date
372	JMD	JCON	Configuration Management Plan, JCON PMO, Version 1.2	Mar 2006
373	JMD	JCON	Contingency Plan, JCON COAR, Version 1.8	Mar 2006
374	JMD	JCON	Contract Administration, JCON	
375	JMD	JCON	Department Executive Review Board Presentation	Feb 2005
376	JMD	JCON	Design and Development Phase Closeout Checklist, JCON SDLC, Version 1.2	
377	JMD	JCON	Implementation Phase Closeout Checklist, Version 1.1, JCON SDLC	
378	JMD	JCON	Implementation Phase Closeout Checklist, Version 1.1, JCON SDLC, (Blank Form)	
379	JMD	JCON	Implementation Plan, EOIR, Final Version 2.7	May 2006
380	JMD	JCON	Initial Privacy Impact Assessment	
382	JMD	JCON	JCON Implementation Plan Template and Guidance, JCON PMO SDLC, Version 2.0	Mar 2005
384	JMD	JCON	JCON SDLC Guide, JCON PMO SDLC, Version 2.0	Mar 2005
385	JMD	JCON	Lessons Learned Report for the JCON Civil Deployment Implementation Phase	May 2006
386	JMD	JCON	Lessons Learned Report Template and Guidance, JCON PMP SDLC, Version 1.0	Jan 2005
387	JMD	JCON	OMB Exhibit 300 for BY 2007	Dec 2005
388	JMD	JCON	Planning Phase Closeout Checklist, JCON SDLC, Version 1.4	
390	JMD	JCON	Privacy Threshold Analysis	
391	JMD	JCON	Project Management Plan Template, JCON PMO SDLC, Version 2.0	May 2005
392	JMD	JCON	Project Management Plan, Civil Rights Division, JCON Implementation	Dec 2005
393	JMD	JCON	Project Management Plan, EOUSA JCON IIA Deployment	May 2005
394	JMD	JCON	Project Management Plan, JCON Modernization	Jun 2005
395	JMD	JCON	Requirements Analysis Phase Closeout Checklist, JCON SDLC, Version 1.2	
398	JMD	JCON	Residual Risk Report for JCON Common Office Automation Resources	May 2006
399	JMD	JCON	Risk Management Areas of Concern	May 2006
400	JMD	JCON	Risk Management Plan, JCON PMO, Version 2	Jul 2003
401	JMD	JCON	Security Test and Evaluation, JCON COAR	May 2006
402	JMD	JCON	Summary of Findings, Email Users Survey	Dec 2005
403	JMD	JCON	System Analysis Report JCON Civil Rights Division Design, Version 1 – Final	Apr 2006

Item ID Number	Component	System or Project	Title	Date
404	JMD	JCON	System Security Plan, JCON-COAR	May 2006
405	JMD	JCON	System Test Plan for DOJ EOIR, Version 1.0, Draft	Aug 2005
406	JMD	JCON	System Test Plan Template, JCON PMO SDLC, Version 1.0	Mar 2005
407	JMD	JCON	Systems Engineering Process, JCON PMO, Version 1.0	Jun 2006
408	JMD	JCON	Vulnerability/Countermeasures and Threat Pairing, JMD, JCON-COAR	May 2006
409	BOP	ITS-II	Security Test and Evaluation Worksheets	
412	BOP	ITS-II	Program Plan	May 2005
413	BOP	ITS-II	Plan of Action and Milestones	
414	BOP	ITS-II	Contingency Plan	Nov 2004
415	BOP	ITS-II	Engineering Management Plan	Apr 2005
416	BOP	ITS-II	Request for Comment	
417	DEA	EPIC	Risk Assessment Report, EPIC	May 2005
419	DEA	EPIC	OCIO: Project Dashboard Project Managers Worksheet, EPIC	
420	DEA	EPIC	System Security Plan, ESS	Aug 2005
421	DEA	EPIC	Action Plan, Independent Evaluation Pursuant to the Federal Information Security Management Act FY 2005, DEA ESS	
422	DEA	EPIC	Contingency Plan, ESS	Mar 2006
423	DEA	EPIC	Training Plan, EPIC Open Connectivity Project	Jun 2004
424	DEA	EPIC	System Engineering Management Plan, EPIC Open Connectivity Project	Jun 2004
425	DEA	EPIC	Configuration Control Board (CCB) Charter and Request for Information Technology Services (RITS) Policy	Feb 2004
426	DEA	EPIC	Verification and Validation Plan, EPIC Open Connectivity Project	Apr 2004
427	DEA	EPIC	NDSS Project, Background: NIBRS/UCR Data, CDX	May 2003
428	DEA	EPIC	General Counterdrug Intelligence Plan	Feb 2000
429	DEA	EPIC	Risk Management Plan, Open Connectivity Project, DEA EPIC, Revised	Aug 2004
430	DEA	EPIC	Feasibility Statement, EPIC Open Connectivity Project,	Apr 2006
431	DEA	EPIC	CONOPS, Connection of the ESS to the EIS, EPIC, Version 1.1	Jun 2004
432	DEA	EPIC	National Drug Seizure System Discussion Paper, CDX	Feb 2004
434	FBI	CARTSAN	CARTSAN Review Network Installation Plan	Jun 2005
435	FBI	CARTSAN	Certification and Accreditation System Registration	Jun 2005
436	FBI	CARTSAN	Certification Test Report, CARTSAN	Aug 2005
437	FBI	CARTSAN	Concept of Operations	

Item ID Number	Component	System or Project	Title	Date
438	FBI	CARTSAN	Configuration Management Plan, Version 0.1 (Draft)	
439	FBI	CARTSAN	Digital Evidence Laboratory Quality Assurance Manual Supplement, CART	Apr 2006
441	FBI	CARTSAN	Earned Value Management Worksheet	Jul 2005
442	FBI	CARTSAN	Guidance on Use of the CAIR Program and Integration with CART Storage Platforms	Aug 2005
443	FBI	CARTSAN	Investment Management/Project Review Board	Aug 2005
444	FBI	CARTSAN	Mission Needs Statement	Nov 2005
446	FBI	CARTSAN	Privacy Impact Assessment, CARTSAN, (Draft)	
447	FBI	CARTSAN	Risk Management Plan	Jul 2005
448	FBI	CARTSAN	Risk Register	Jul 2005
449	FBI	CARTSAN	System Security Plan, CARTSAN	Aug 2005
450	FBI	CARTSAN	Top Level Tasks, CARTSAN Phase One	Jul 2006
454	FBI	BRIDG	Concept of Operations, DHS/US-VISIT and DOJ/FBI Interoperability, iDSM, Final	Apr 2006
455	FBI	BRIDG	Full Business Case, IDENT-IAFIS Interoperability, iDSM Project	Jan 2006
456	FBI	BRIDG	iDSM, WBS, CJIS Bridge	Jul 2006
457	FBI	BRIDG	Mission Needs Statement, iDSM, Version 1.2	Jan 2006
458	FBI	BRIDG	Open Risks Worksheet, iDSM	Jun 2006
459	FBI	BRIDG	Privacy Impact Assessment for the DOJ/FBI-DHS Interim Data Sharing Model (iDSM)	
460	FBI	BRIDG	Project Health Assessment, iDSM, Gate 1 & 2	Feb 2006
461	FBI	BRIDG	Project Health Assessment, iDSM, Gate 3 (Final Design)	Jun 2006
462	FBI	BRIDG	Risk Management Plan, iDSM Project	Jan 2006
463	FBI	CODIS	Acquisition Strategy Review, CODIS 6.0	Oct 2005
464	FBI	CODIS	CODIS Accreditation Decision	Apr 2005
465	FBI	CODIS	Combined DNA Index System Mission Needs Statement	Nov 2005
466	FBI	CODIS	CODIS Schedule	
467	FBI	CODIS	FY 2008 Full Business Case	Dec 2005
468	FBI	CODIS	Independent Assessment Findings and Recommendations, CODIS, Final	Jun 2005
469	FBI	CODIS	Description of Current CODIS Architecture	
470	FBI	CODIS	Plans of Actions and Milestones, CODIS	Feb 2005
471	FBI	CODIS	Privacy Impact Assessment, National DNA Index System (NDIS) Database	Oct 2004
472	FBI	CODIS	Product Management Plan, CODIS Bridge Contract Extension	Sep 2005
473	FBI	CODIS	Risk Management Plan, CODIS, Draft Version 01	May 2006
474	FBI	CODIS	Risk Register, CODIS, Open Risks Worksheet	Feb 2006

Item ID Number	Component	System or Project	Title	Date
475	FBI	CODIS	Single Acquisition Management Plan for the Combined DNA Index System	Feb 2006
476	FBI	CODIS	System Security Plan, CODIS	Jan 2005
477	FBI	CODIS	Three Part Contingency Plan, CODIS Bridge Contract Extension	Oct 2005
478	FBI	DCU	Action Plan, Enterprise Servers (Administrative and Investigative Mainframes), Secret (Working Draft)	Jul 2004
479	FBI	DCU	Approval to Operate for the Investigative Mainframe Application (IMA)	May 2006
480	FBI	DCU	Continuity of Operations Plan, FBI, ITOD, Operations Section	Jan 2005
481	FBI	DCU	Contribution of the Mainframe to the Bureau's Mission, FBI	Feb 2006
483	FBI	DCU	Investment Evaluation Form, IT Management	May 2006
484	FBI	DCU	ITOD Hardware Review, Executive Dashboard (Draft)	Mar 2006
485	FBI	DCU	Mainframe Hardware Test Environment	
486	FBI	DCU	Mission Needs Statement, Enterprise Backup Project	Jul 2005
487	FBI	DCU	OMB Exhibit 300 for BY 2005	
488	FBI	DCU	OMB Exhibit 300 for BY 2007	Jul 2005
489	FBI	DCU	OMB Exhibit 300 for BY 2008	Jul 2005
490	FBI	DCU	Project Plan, Global Mirroring Project	Dec 2005
491	FBI	DCU	Project Summary Report, ITOD Mainframe System Upgrade	
492	FBI	DCU	System Security Plan, FBI, Enterprise Servers, Version 1.2	Oct 2004
493	FBI	DCS	Benefits & Cost Analysis Project Synopsis, DCS-5000 Regional Architecture, Step 4 and 5	Feb 2006
494	FBI	DCS	Benefits & Cost Analysis Project, DCS-5000 Regional Architecture, Step 2 and 3	Nov 2005
495	FBI	DCS	Benefits & Cost Analysis Project, DCS-5000 Regional Architecture, Step 4 and 5	Jan 2006
496	FBI	DCS	Configuration Management Plan, DCS-6000, Appendix O	May 2006
497	FBI	DCS	DCS-5000 Accreditation Decision - Grant ATO for DCS-5000, IT System Security Risk Analysis	Feb 2006
498	FBI	DCS	DCS-5000 Schedule	
499	FBI	DCS	DCS-6000 - Grant ATO with Conditions, IT Systems Security Risk Analyses	May 2006
500	FBI	DCS	DCS-6000 Accreditation Decision - Security Characteristic and Tier Level Designation for DCS-6000, IT Systems Security Risk Analyses	May 2006
501	FBI	DCS	DCS-6000 Schedule, Appendix B (Table)	

Item ID Number	Component	System or Project	Title	Date
509	FBI	DCS	Phase Review Report, Phase 1/2, Project Digital Storm,	Aug 1998
510	FBI	DCS	Privacy Impact Assessment, SPIDERNET and DIGITAL STORM	Aug 2001
511	FBI	DCS	Privacy Impact Assessment, Upgrade from SPIDERNET to Red Wolf	Dec 2005
514	FBI	DCS	Project Closeout Report, Digital Collection-04, Version 1.1	Jul 2005
516	FBI	DCS	Project Plan, Digital Collection System, Digital Collection -05	Nov 2004
517	FBI	DCS	Project Plan, Digital Collection, Digital Collection -03	Aug 2003
518	FBI	DCS	Project Plan, Digital Collection, Digital Collection -04	Jan 2004
519	FBI	DCS	Project Plan, Digital Storm	Jun 1998
520	FBI	DCS	Project Status Report, DCS-5000	Jun 2006
521	FBI	DCS	Risk Assessment and Management Plan (RAMP), DCS-6000, Systems Security Plan, Appendix L, Version 2.0	May 2006
522	FBI	DCS	Security Concept of Operations, DCS-6000, Appendix S, Version 1.0	May 2006
523	FBI	DCS	Statement of Need, Digital Delight	Jan 1997
524	FBI	DCS	System Security Plan, DCS 3000, Version 2.0	Apr 2006
525	FBI	DCS	System Security Plan, DCS-5000, Revision 3.5	Dec 2005
526	FBI	DCS	System Security Plan, DCS6000 Voice Box III, Version 3.1	May 2006
527	FBI	DCS	Test Plan, Digital Storm, Version 1.0	Feb 1999
528	FBI	DCS	Work Breakdown Structure (WBS) for Project Digital Storm, Version 1.0	Mar 1998
529	FBI	EDMS	Privacy Impact Assessment (PIA), Draft	Sep 2005
530	FBI	EDMS	Certification Decision, Recommendation for ATO for ITD/EIMO/EDMS	Jun 2004
531	FBI	EDMS	Certification Test Plan	Apr 2004
532	FBI	EDMS	Configuration Management Plan, Revision b	Sep 2005
533	FBI	EDMS	Continuity of Operations Plan	Apr 2004
535	FBI	EDMS	Department Investment Review Board	
536	FBI	EDMS	EDMS Briefing for the FBI Science and Technology Advisory Board	Jul 2005
537	FBI	EDMS	Installation Plan, EDMS	
538	FBI	EDMS	EDMS, ELSUR Data Management System Background/History	
540	FBI	EDMS	OMB Exhibit 300 for BY 2007	Sep 2005
542	FBI	EDMS	Independent Government Cost Estimate, Next Generation Electronic Surveillance, Data Management System	Nov 2005

Item ID Number	Component	System or Project	Title	Date
543	FBI	EDMS	Monthly Project Status Reporting	Dec 2005
544	FBI	EDMS	Project Plan, Project EDMS (ELSUR Data Management System)	Feb 2004
545	FBI	EDMS	Master Schedule, EDMS	
546	FBI	EDMS	Project Status Report, ELSUR EDMS	Apr 2006
547	FBI	EDMS	Risk Management Plan, EDMS	Aug 2000
548	FBI	EDMS	Risk Management Plan, EDMS, version 3.0	
549	FBI	EDMS	Proposed Risk Worksheets	
550	FBI	EDMS	Statement of Need, Phase 1, Information Management System (IMS)	Jan 1998
551	FBI	EDMS	Strategic Training Plan	Jun 2005
552	FBI	EDMS	System Concept of Operations, EDMS, version 1.2	Feb 2004
553	FBI	EDMS	System Security Plan, EDMS, version EDMS SSP Rev. 2.0	Apr 2004
554	FBI	EDMS	Target EA and Transition, EDMS Enterprise Architecture, Executive Summary, V1.0	Jan 2005
555	FBI	EDMS	Test and Evaluation Master Plan, EDMS, Revision A	Aug 2005
558	FBI	FTTTF	Concept of Operations (CONOPS), Guardian 2.0, Version 1.0	Mar 2006
559	FBI	FTTTF	Concept of Operations, DEEP, Revision 0.3	Sep 2004
560	FBI	FTTTF	Critical Performance Measures, Guardian 2, Version 1.0	Apr 2006
561	FBI	FTTTF	Installation Plan, Guardian 2, Draft Version 5.0	Apr 2006
562	FBI	FTTTF	Mission Need Statement, Guardian 2, Version C	Jan 2006
563	FBI	FTTTF	Project Charter, CTD Data Extraction and Extension Project (DEEP)	Jul 2004
564	FBI	FTTTF	Project Management Plan (Software Development Plan), Guardian 2.0, Version 9.0	Mar 2006
565	FBI	FTTTF	Risk Management Plan, Guardian, Version 1.0	Apr 2006
566	FBI	FTTTF	Risk Register Worksheet, Guardian	Mar 2006
567	FBI	FTTTF	System Engineering Management Plan, Guardian, Draft Version 11.0	Mar 2006
568	FBI	FTTTF	Test and Evaluation Master Plan, Guardian, Version 1.0	Mar 2006
569	FBI	FTTTF	Test Procedures, DEEP, Release 1.2	Sep 2005
570	FBI	FTTTF	Test Procedures, DEEP, Version 1	
571	FBI	FTTTF	Test Procedures, Guardian, Version 7.0	Apr 2006
573	FBI	IAFIS	Build C Test Report, Volume 1	Aug 1997
574	FBI	IAFIS	Build D Installation Plan	Nov 1997
575	FBI	IAFIS	Build D Test Report, Volume 1	Dec 1997
576	FBI	IAFIS	Build E Installation Plan	Apr 1998

Item ID Number	Component	System or Project	Title	Date
577	FBI	IAFIS	Build E System Integration and Test Plan (SITP), IAFIS	Jan 1998
578	FBI	IAFIS	Build E Test Report, Volume 2	May 1998
579	FBI	IAFIS	Build F Installation Plan	Mar 1998
580	FBI	IAFIS	Build F Installation Plan (CWV Draft 3, as Built)	Jun 2000
581	FBI	IAFIS	Build F1 Test Report, Volume 1	May 1999
582	FBI	IAFIS	Configuration Management Plan, Criminal Justice Information Services Division, Revision1.2	Aug 2002
583	FBI	IAFIS	Early Build C Installation Plan	May 1997
584	FBI	IAFIS	IAFIS System Acceptance Test Plan, Volume 1	Feb 1999
585	FBI	IAFIS	IAFIS System Acceptance Test Report	Aug 1999
586	FBI	IAFIS	Independent Verification, Validation & Testing (IVV&T) SOW, CJIS Division	Nov 1993
587	FBI	IAFIS	ITN Training Plan	Jul 1999
588	FBI	IAFIS	Operational System Security Plan, AFIS	Jan 1999
589	FBI	IAFIS	Quality Assurance Plan, CJIS Division	Mar 2005
591	FBI	IAFIS	System Security Plan, IAFIS, Version 2.1	Mar 2006
592	FBI	IAFIS	Systems Engineering Management Plan, Criminal Justice Information Services Division	Jul 2005
593	FBI	IAFIS	Systems Engineering Management Plan, SoSSS, Revision 2.2 Final	Nov 2005
594	FBI	IAFIS	Technical Data Collection Tool, CJIS Division (spreadsheet)	
595	FBI	IAFIS	Training Plan, AFIS	Nov 1998
596	FBI	IAFIS	Transition Plan, IAFIS, Second Iteration	Apr 1998
597	FBI	IAFIS	Transition Plan, IAFIS, Third Iteration	Oct 1998
598	FBI	IATI	CARA WBS	
599	FBI	IATI	CARA Technical Review Board Briefing	May 2006
600	FBI	IATI	Concept of Operations, FBI IATI Program, CARA	Apr 2005
601	FBI	IATI	Concept of Operations, FBI IATI Program, IODM, Version 1.0	Sep 2005
602	FBI	IATI	Configuration Management Plan (CMP), Technology Infusion Program (TI), Volume 1, Version 0.5	Nov 2003
604	FBI	IATI	Earned Value Management Report, IATI Program, Version 1.0	May 2006
605	FBI	IATI	Feasibility Study, IATI Program, CARA, Version 1.0	Mar 2005
606	FBI	IATI	IATI Green Book Report	Jun 2006
608	FBI	IATI	Installation Plan, IATI Program, IODM, Version 2.0	May 2006
609	FBI	IATI	IODM WBS	
610	FBI	IATI	IODM, Technical Review Board Briefing	Jan 2006
611	FBI	IATI	Mission Needs Statement, IATI	

Item ID Number	Component	System or Project	Title	Date
612	FBI	IATI	OMB Exhibit 300 for FY 2008	Mar 2006
613	FBI	IATI	Privacy Impact Assessment, CARA	Apr 2006
614	FBI	IATI	Program Management Plan, Technology Infusion Program, Volume I, Version .19	Nov 2003
615	FBI	IATI	Quality Assurance Plan (QAP), IATI, Volume 1, Version .9	Nov 2003
616	FBI	IATI	Risk Management Plan (RMP), Technology Infusion Program, Version .8	Nov 2003
617	FBI	IATI	Risk Worksheet, CARA	May 2006
618	FBI	IATI	Risk Worksheet, IODM	Mar 2006
619	FBI	IATI	Security Attachment to the FBI System Security Plan (SSP), IATI Program, IODM, Version 2.0	May 2006
621	FBI	IATI	System Engineering Master Plan, IATI Program, Version 1.0	May 2004
622	FBI	IATI	System Installation Plan, IATI Program, CARA, Version 3.0	May 2006
623	FBI	IATI	System Security Plan (SSP), IATI Program, CARA, Version 6.0	May 2006
624	FBI	IATI	System Security Plan (SSP), IATI, SSIAC, SAE, Version 7.0	Mar 2006
625	FBI	IATI	System Test Plan, IATI Program, CARA, Version 3.0	Jan 2006
626	FBI	IATI	Test and Evaluation Master Plan (TEMP), IATI, Draft	Apr 2004
627	FBI	IATI	Test Plan, IATI Program, IODM, Version 3.0	May 2006
628	FBI	IATI	Training Plan, IATI Program, CARA, Version 2.0	Apr 2006
629	FBI	IATI	Transition Plan, IATI Program, CARA, Version1.0	May 2006
630	FBI	IDW	ORACLE 9.2.0.4 Upgrade Plan	
631	FBI	IDW	Risk Management Plan, IDW, Version 1.0	Feb 2005
632	FBI	IDW	Risk Register, IDW (Spreadsheet)	Dec 2005
633	FBI	IDW	System Security Plan, IDW, Version 2.0	May 2006
634	FBI	IDW	Test & Evaluation Test Analysis Report (TETAR) for IDW, Version 1.1	Jul 2004
635	FBI	IDW	Training Management Plan, IDW	Jun 2004
636	FBI	IDW	Transition and Deployment Plan, IDW	Jun 2004
637	FBI	LEO	Appendix C: Test Cases and Scenarios, Workflow Part 1 (Final Draft)	Jun 2006
638	FBI	LEO	Appendix C: Workflow Part 2 (Final Draft)	Jun 2006
639	FBI	LEO	Appendix C: Workflow Part 3 (Final Draft)	Jun 2006
640	FBI	LEO	Control Gate 4 & 5, LEO Reengineering/Relocate, Project Health Review	Jun 2006
641	FBI	LEO	Earned Value Management Variances, LEO	May 2006
642	FBI	LEO	FBI LEO System Security Plan, dated 9 June 2006	Jun 2006

Item ID Number	Component	System or Project	Title	Date
643	FBI	LEO	Implementation Plan for the LEO System Relocation of Primary Operations to the CJIS Division	May 2006
644	FBI	LEO	Installation Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Dec 2005
645	FBI	LEO	IT Contingency Plan, LEO, Version 1.0 (Draft)	May 2006
646	FBI	LEO	LEO CM Working Group Schedule	Jun 2004
647	FBI	LEO	LEO Configuration Management (CM) Processes, dated 21 June 2004	Jun 2004
649	FBI	LEO	Project Implementation Schedule	
650	FBI	LEO	Project Implementation Schedule (Draft)	Apr 2006
651	FBI	LEO	Project Implementation Schedule, Appendix B (Draft)	Apr 2006
652	FBI	LEO	Project Implementation Schedule, Appendix C	
653	FBI	LEO	Project Management Plan, LEO, Relocation and Reengineering Project	Jun 2006
655	FBI	LEO	Requirements Traceability Matrix (RTM) for the LEO System Relocation of Primary Operations to the CJIS Division (Draft)	Jun 2006
656	FBI	LEO	Risk Register	Jun 2006
657	FBI	LEO	System Test Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Jun 2006
658	FBI	LEO	Test Readiness Review, LEO Relocation	Jun 2006
659	FBI	LEO	Transition Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Jun 2006
660	FBI	R-DEx	Certification Test Plan, R-DEx, Version 1.6	Feb 2005
661	FBI	R-DEx	Certification Test Report, R-DEx, Version 1.6	Feb 2005
662	FBI	R-DEx	Risk Assessment and Risk Management Matrix (RMM), R-DEx, Version 1.0	Jul 2005
663	FBI	R-DEx	Security Requirements Traceability Matrix (SRTM), Version 1.0	Mar 2004
664	FBI	R-DEx	System Security Plan, FBI Regional Data Exchange (R-DEx), Version 4.2	May 2006
665	FBI	NCIC	External Interface Checkout Test Report for NCIC 2000	May 1999
668	FBI	NCIC	Concept of Operations, CJIS, NCIC 2000/IAFIS Interface	Aug 1995
669	FBI	NCIC	Configuration and Data Management Plan for NCIC 2000	Feb 1998
670	FBI	NCIC	Facility Requirements and Installation Plan for NCIC 2000	Jul 1998
672	FBI	NCIC	Fingerprint Matching Subsystem Beta Test Report, NCIC 2000	May 1999
673	FBI	NCIC	FMS Reintegration Test Report for NCIC 2000	Mar 1999

Item ID Number	Component	System or Project	Title	Date
674	FBI	NCIC	Interim Disaster Recovery Concept of Operations, CJIS Division Information Technology Management Section, NCIC	Jun 2003
675	FBI	NCIC	Maintainability Test Plan and Procedure for NCIC 2000	May 1999
676	FBI	NCIC	Maintainability Test Plan for NCIC 2000	Feb 1994
677	FBI	NCIC	Maintainability Test Report for NCIC 2000	Jun 1999
678	FBI	NCIC	NCIC 2000 Security Certification and Testing Analysis	Jul 1999
679	FBI	NCIC	NCIC 2000 Segment	Jun 1994
680	FBI	NCIC	NCIC 2000 Segment	May 1994
681	FBI	NCIC	Personnel Requirements and Training Plan for NCIC	Nov 1998
682	FBI	NCIC	Plan for Early Delivery of the FMS Subsystem, NCIC 2000 Program	Apr 1997
683	FBI	NCIC	Risk Analysis of the NCIC 2000, Working Paper	Oct 1989
684	FBI	NCIC	Risk Management Plan for NCIC 2000, Revision 2	Feb 1996
685	FBI	NCIC	Security Certification Status Report	Jun 1998
686	FBI	NCIC	Successive Level Integration Test Plan for NCIC 2000	Jul 1996
687	FBI	NCIC	System Engineering Management Plan for NCIC 2000	May 1996
688	FBI	NCIC	System Security Plan (SSP), NCIC	Jul 2006
689	FBI	NCIC	Technical Data Collection Tool, CJIS Division, NCIC (spreadsheet)	
690	FBI	NCIC	Test and Evaluation Master Plan for NCIC 2000	Mar 1996
691	FBI	NCIC	Transition Plan for NCIC 2000	Aug 1998
693	FBI	NCIC	Preliminary Transition Plan for NCIC,Volume I of VII, Transition Overview	Apr 1997
694	FBI	N-DEx	Certification Test Plan, N-DEx	Oct 2004
695	FBI	N-DEx	Concept of Operations, Law Enforcement National Data Exchange (N-DEx), Version 1.5	May 2006
697	FBI	N-DEx	Mission Needs Statement, Law Enforcement National Data Exchange (N-DEx), Version 1.0	Dec 2005
699	FBI	N-DEx	Program Plan, Law Enforcement N-Dex	Jul 2006
700	FBI	N-DEx	Risk Management Plan, Law Enforcement N-DEx, Version 1.4	Aug 2006
701	FBI	N-DEx	Risk Register Worksheet, N-DEx	Jun 2006
702	FBI	N-DEx	System Security Plan Attachment H - Risk Assessment, N-Dex Prototype, Version 1.1	Jun 2004
703	FBI	NGI	Concept of Operations, NGI Advanced Fingerprint Identification Technology Component	Jan 2006
704	FBI	NGI	Concept of Operations, NGI Disposition Reporting Improvements Component	Jun 2006

Item ID Number	Component	System or Project	Title	Date
705	FBI	NGI	Concept of Operations, NGI Enhanced IAFIS Repository Component	Jan 2006
706	FBI	NGI	Concept of Operations, NGI Interstate Photo System Enhancements Component	Jan 2006
707	FBI	NGI	Concept of Operations, NGI National Palm Print System Component	Jan 2006
708	FBI	NGI	Concept of Operations, NGI Quality Check Automation Component	Jan 2006
709	FBI	NGI	Configuration Management Plan, NGI	Apr 2006
710	FBI	NGI	Investment Management/Project Review Board (IMPRB), Summary Notes	Apr 2005
711	FBI	NGI	Earned Value, Template for Monthly Project Status Reporting	
713	FBI	NGI	Investment Management/Project Review Board	Feb 2006
714	FBI	NGI	Cost Benefit Analysis Worksheet	
715	FBI	NGI	Milestone Report, NGI Requirements Analysis, Draft Rebaseline 2	May 2006
716	FBI	NGI	Mission Needs Statement, NGI, Final, Version 1.0	Apr 2006
719	FBI	NGI	PIA, Advanced Fingerprint Identification Technology (AFIT)	
720	FBI	NGI	PIA, Enhanced IAFIS Repository	
721	FBI	NGI	PIA, Interstate Photo System (IPS)	
722	FBI	NGI	PIA, National Palm Print System (NPPS)	
725	FBI	NGI	Program Management Review	May 2006
726	FBI	NGI	Project Management Plan, NGI, Version 1.0	Jan 2006
727	FBI	NGI	Quality Assurance Plan, NGI	May 2006
728	FBI	NGI	Risk Register, NGI	May 2006
729	FBI	NGI	Risk Management Plan, NGI	Nov 2005
730	FBI	NICS	Certification Test Plan, NICS/E-Checks/NICS Call Center	Sep 2005
731	FBI	NICS	Concept of Operations, NICS Efficiency Upgrade Project	Mar 2003
732	FBI	NICS	Configuration Management Plan, CJIS Division, Revision 1.2	Aug 2002
733	FBI	NICS	Contingency Plan, NICS	Dec 2001
735	FBI	NICS	Contingency Plan, NICS and E-Check	Sep 2005
737	FBI	NICS	Formal Qualification Test Plan, NICS	Jul 1998
739	FBI	NICS	Formal Qualification Test Report, NICS	Oct 1998
740	FBI	NICS	Installation Plan, NICS	Jun 1998
741	FBI	NICS	NICS Efficiency Upgrade Installation Plan, Draft	Sep 2003
742	FBI	NICS	NICS Rehost Transition Plan	May 2004

Item ID Number	Component	System or Project	Title	Date
743	FBI	NICS	Quality Assurance Plan, CJIS Division	Mar 2005
744	FBI	NICS	Security Requirements Traceability Matrix, NICS	
745	FBI	NICS	Superdome System Administration and Installation Cookbook, NICS [Rehost]	Jul 2005
746	FBI	NICS	System Security Plan, NICS/ FBI	May 1998
747	FBI	NICS	System Test Plan, NICS Efficiency Upgrade Project, Draft	Jun 2003
748	FBI	NICS	System Tests, NICS	
749	FBI	NICS	Transition Plan NICS Efficiency Upgrade Project	Oct 2003
750	FBI	NICS	Windows 2003 Server Installation Cookbook, NICS, Revision 3.0 [Efficiency Upgrade]	Mar 2006
751	FBI	SCION	Full Privacy Impact Assessment, TS/SCI LAN	Dec 2002
752	FBI	SCION	Configuration Management Plan, SCION	Dec 2003
753	FBI	SCION	System Security Plan, SCION	Aug 2004
754	FBI	SCION	Certification Test Results, TS/SCI LAN	May 2003
755	FBI	Sentinel	Acquisition Plan (FD-911), SENTINEL, Version 2.0	Aug 2005
757	FBI	Sentinel	Communication Plan, SENTINEL, Version 1.0	Sep 2005
758	FBI	Sentinel	Configuration Management Plan, SENTINEL PMO, Version 1.1	Jul 2005
759	FBI	Sentinel	Deliverables, SENTINEL SOW, Attachment 2	
760	FBI	Sentinel	IMPRB Acquisition Plan Review, Gate 2 Signatures	Jul 2005
761	FBI	Sentinel	Incremental Development Plan (IDP), SENTINEL,	Jul 2005
762	FBI	Sentinel	Investment Evaluation Form, Gate 1 Signatures	Jul 2005
763	FBI	Sentinel	Meeting Minutes, Contract Implementation Review (CIR)-Part 1	Mar 2006
764	FBI	Sentinel	Meeting Minutes, Contract Implementation Review (CIR)-Part 2	Apr 2006
765	FBI	Sentinel	Meeting Minutes, Requirements Clarification Review (RCR), Version 1.0	May 2006
766	FBI	Sentinel	Mission Needs Statement	Jul 2005
769	FBI	Sentinel	Risk Register, SENTINEL	Jun 2006
770	FBI	Sentinel	Program Management Plan, SENTINEL, Version 1.2	Aug 2005
771	FBI	Sentinel	Quality Management Plan, SENTINEL, Version 1.0	Jul 2005
772	FBI	Sentinel	Risk Management Plan, SENTINEL, Version 1.2	Jul 2005
773	FBI	Sentinel	Source Selection Decision Document for SENTINEL	Mar 2006
775	FBI	Sentinel	System Concept of Operations, SENTINEL, Version 1.1	Jul 2005
776	FBI	Sentinel	Systems Engineering Management Plan (SEMP), SENTINEL	Jun 2005
777	FBI	Sentinel	Test and Evaluation Master Plan (TEMP), SENTINEL	Jul 2005

Item ID Number	Component	System or Project	Title	Date
778	FBI	SMIS	90 Day Evaluation Pilot, FDF Automation System User Requirements for FBI Security Divisions	Jan 2005
782	FBI	SMIS	Certification Test Plan, FDF-A	Jan 2006
783	FBI	SMIS	Certification Test Report, FDF-A	Feb 2006
784	FBI	SMIS	Concept of Operations, FBI SMIS, Version 2.0	Dec 2004
785	FBI	SMIS	Configuration Management Plan, SMIS, PMO, Version 1.0	Jul 2005
786	FBI	SMIS	Control Gate Review Exit Report, SMIS, FDF-A, Gate 6 - OAR	Mar 2006
788	FBI	SMIS	Cost Benefit Analysis, FDF-A, (Spreadsheet)	
791	FBI	SMIS	Initial Privacy Impact Assessment, Polygraph Workflow Management Application	Aug 2005
792	FBI	SMIS	Initial Privacy Impact Assessment, SMIS	Aug 2005
793	FBI	SMIS	Investment Management/ Project Review Board (IMPRB), Summary Notes	Aug 2005
794	FBI	SMIS	Investment Management/ Project Review Board (IMPRB), Summary Notes	Jan 2005
797	FBI	SMIS	OMB Exhibit 300 for BY 2007	Jan 2006
798	FBI	SMIS	Privacy Impact Assessment, Security Division Implementation the Financial Disclosure Forms Analyzer	Feb 2006
799	FBI	SMIS	Project Health Review, SMIS, FDF-A, Gate 2 Approval	Mar 2006
800	FBI	SMIS	Project Management Review, SMIS	Jan 2006
801	FBI	SMIS	Project Management Review, SMIS	Feb 2006
802	FBI	SMIS	Project Management Review, SMIS	Mar 2006
803	FBI	SMIS	Project Management Review, SMIS	Dec 2005
804	FBI	SMIS	Project Management Review, SMIS	Nov 2005
805	FBI	SMIS	Project Management Review, SMIS	Apr 2005
806	FBI	SMIS	Project Management Review, SMIS	Jul 2005
807	FBI	SMIS	Project Management Review, SMIS	Jun 2005
808	FBI	SMIS	Project Management Review, SMIS	May 2005
809	FBI	SMIS	Project Management Review, SMIS	Oct 2005
810	FBI	SMIS	Project Management Review, SMIS	Sep 2005
811	FBI	SMIS	Project Management Review, SMIS	May 2006
812	FBI	SMIS	Project Plan, SMIS Facilities Certification and Accreditation Component, Draft	Mar 2006
813	FBI	SMIS	Project Plan, SMIS Financial Disclosure Forms Analyzer Component, Draft	Feb 2006
814	FBI	SMIS	Project Plan, SMIS, Version 0.7, Draft	Jul 2005
815	FBI	SMIS	Quality Management Plan, SMIS, Version 1.0	Jul 2005
816	FBI	SMIS	Risk Management Matrix, FDF-A, Version 1.0	Feb 2006

Item ID Number	Component	System or Project	Title	Date
817	FBI	SMIS	Risk Management Plan, SMIS, Final 1.1	Dec 2005
818	FBI	SMIS	Risk Register, SMIS	Mar 2006
819	FBI	SMIS	Security Concept of Operations for the Automated Facilities Management System for Facilities Certification and Accreditation	May 2006
820	FBI	SMIS	Security Concept of Operations, Polygraph Workflow Management Application	Oct 2005
823	FBI	SMIS	SMIS Master Schedule	
825	FBI	SMIS	System Concept of Operations, E-Disclose	
826	FBI	SMIS	System Security Plan, Financial Disclosure Forms Analyzer (FDF-A), Version 1.2	Jan 2006
827	FBI	SMIS	System Security Plan, Polygraph Workflow Management System	Apr 2006
828	FBI	SMIS	Test Analysis Report for the Polygraph Workflow Management Application	Nov 2005
829	FBI	SMIS	Test and Evaluation Master Plan for the Polygraph Workflow Management Application	Aug 2005
830	FBI	SMIS	Test Procedure Results, PWMA	Nov 2005
831	FBI	SMIS	Testing and Evaluation Master Plan Unit Testing and Traceability Matrix, SMIS FCA Application	Mar 2006
832	FBI	SMIS	Threat Assessment Report, FDF-A	Feb 2006
833	FBI	SMIS	Training Plan for the Polygraph Workflow Management Application	Sep 2005
835	FBI	TRP	IT Maintenance & Licensing Dashboard	Jun 2006
836	FBI	TRP	Project Summary Report, TRP	Dec 2006
838	FBI	TSC	Deployment Plan	Feb 2006
839	FBI	TSC	ATO The TSC Terrorist Screening Database 1B System (TSDB-1B)	Dec 2004
840	FBI	TSC	IT Risk Management Matrix, TSC	
842	FBI	TSC	IV & V Test Procedures for TSDB 1.8.0.2, TSC	
843	FBI	TSC	IV & V Test Report, TSDB 1.8.0.2, TSC	May 2006
844	FBI	TSC	Project Schedule TSDB 1 8 Mar	Jun 2006
845	FBI	TSC	Risk Management Plan, Terrorist Screening Center (TSC), Version 1.7 (Draft)	Apr 2006
846	FBI	TSC	System Security Plan, TSDB Phase 1B, Version 1.2	Jul 2005
847	FBI	TSC	Test Management Plan, TSDB 1.7.1	Mar 2006
848	FBI	TSC	Independent Verification and Validation (IV &V) Plan, TSC	
849	FBI	TSC	TSDB Automated Ingest Project Plan	Apr 2006
850	FBI	TSC	Template for Monthly Project Status Report	
851	EOIR	eWorld	Project Management Plan, CASE Court Pilot	Apr 2006

Item ID Number	Component	System or Project	Title	Date
852	EOIR	eWorld	Project Management Plan, Digital Audio Recording Project, Version 0.05	May 2006
853	EOIR	eWorld	Project Management Plan, Immigration Review Information Exchange System Phase 1 Design (Draft)	May 2006
854	EOIR	eWorld	Market Survey, EOIR, Digital Audio Recording Project, Version 0.16 (Draft)	Apr 2006
855	EOIR	eWorld	IT Contingency Plan, EOIR, JCON-II/CASE, Version 2.0	Nov 2005
856	EOIR	eWorld	Configuration Management Plan, EOIR	Mar 2006
857	EOIR	eWorld	Configuration Management Plan, eWorld, Version 1.0 (Draft)	Feb 2006
860	EOIR	eWorld	Privacy Impact Assessment, Executive Office for Immigration Review	Apr 2006
862	EOIR	eWorld	OCIO: Project Dashboard	
863	EOIR	eWorld	System Security Plan (SSP) for JCON-II/CASE, EOIR	Mar 2006
864	EOIR	eWorld	DOJ Validation Test Script Forms, JCON-II/CASE	
865	EOIR	eWorld	System Security Policy, EOIR, JCON-II/CASE Network	Nov 2005
867	EOIR	eWorld	Incident Response Plan for JCON-II/CASE, EOIR, Version 2.1	Feb 2006
868	EOIR	eWorld	Request for Approval of EOIR Quality Assurance Guidelines	Jun 2006
1004	JMD	IWN	Strategic Plan 2005-2010, Integrated Wireless Network (IWN), (Draft)	Jun 2006
1005	JMD	JCON	Strategic and Tactical Plan, JCON	Apr 2005
1008	JMD	PKI	Project Plan Schedule	
1012	JMD	JCON	Request for Information (RFI), JCON PMO, Version 1.0	Apr 2006
1013	ODAG	OFC	Project Schedule, Milestones (Spreadsheets)	
1014	ODAG	OFC	Project Schedule (Spreadsheets)	
1017	FBI	LEO	OMB Exhibit 300 for BY 2008, CEI	
1017	JMD	PKI	OMB Exhibit 300 for BY 2008, CEI	
1021	DEA	Firebird	Security Operating Procedures Guide, Firebird (FSOPG), Version 4.0	Mar 2004
1022	DEA	M204	Events WBS CY 2004	Dec 2006
1023	FBI	CARTSAN	OMB Exhibit 300 for BY 2008	Dec 2006
1024	FBI	DCS	OMB Exhibit 300 for BY 2008	Aug 2006
1025	FBI	EDMS	OMB Exhibit 300 for BY 2008	Aug 2006
1026	FBI	FTTTF	OMB Exhibit 300 for BY 2008	Dec 2006
1027	FBI	IAFIS	OMB Exhibit 300 for BY 2008	Aug 2006
1028	FBI	NCIC	OMB Exhibit 300 for BY 2008	Aug 2006
1029	FBI	N-DEx	OMB Exhibit 300 for BY 2008	Dec 2006

Item ID Number	Component	System or Project	Title	Date
1030	FBI	NGI	OMB Exhibit 300 for BY 2008	Aug 2006
1031	FBI	NICS	OMB Exhibit 300 for BY 2008	Dec 2006
1032	FBI	R-DEx	OMB Exhibit 300 for BY 2008	Dec 2006
1033	FBI	Sentinel	OMB Exhibit 300 for BY 2008	Aug 2006
1034	FBI	TRP	OMB Exhibit 300 for BY 2008	Dec 2006
1035	FBI	TSC	OMB Exhibit 300 for BY 2008	Dec 2006
1036	FBI	BRIDG	OMB Exhibit 300 for BY 2008	Aug 2006
1037	FBI	Sentinel	Source Selection Plan, FBI Sentinel Program, Version 2.95	Aug 2005
1038	FBI	Sentinel	Statement of Work, Sentinel, Version 2.1	Aug 2005
1039	FBI	Sentinel	Lessons Learned, Sentinel, Version 1.0	Jul 2005
1369	ODAG	OFC	Third Party Tool Recommendations	Jun 2005
1370	ODAG	OFC	Background Comp Analysis	
1371	ODAG	OFC	Draft Comparative Analysis of OCDETF Requirements with Existing DOJ Data Warehousing Efforts	Apr 2003
1372	ODAG	OFC	Comparative Analysis of the FBI's SCOPE and FTTTF	Apr 2003
1374	ODAG	OFC	FTTTF Tech Concept of OPS	Feb 2003
1375	ODAG	OFC	SCOPE Functional Requirements with NEDRS Comparison	
1376	ODAG	OFC	Survey of Data Warehousing Tools - FTTTF, NEDRS	Mar 2004
1377	ODAG	OFC	Comparative Analysis of the FBIs SCOPE and DEAs NEDRS Systems	Feb 2003
1378	DEA	Firebird	OMB Exhibit 300 for BY 07	Sep 2005
1379	DEA	Firebird	Firebird Information Technology Support (FITS) Market Research Report	Mar 2004
1380	DEA	Firebird	Firebird Information Technology Support (FITS) Acquisition Strategy Executive Summary	Mar 2004
1383	JMD	LCMS	Privacy Impact Assessment (Draft)	May 2005
1384	DEA	Merlin	Security Test & Evaluation Plan and Procedures	Aug 2003
1385	DEA	Merlin	Certification Results	Aug 2003
1386	FBI	N-Dex	Privacy Impact Assessment, N-Dex	Mar 2006
1387	FBI	N-Dex	Project Schedule, N-Dex	
1388	JMD	IWN	Market Research Summary	Apr 2004
1389	JMD	IWN	Concept of Operations, IWN	
1390	OJP	JGMS	Validation Test Script Forms, GMS	Feb 2006
1392	BOP	ITS-II	OMB Exhibit 300 BY 2006	
1394	DEA	M204	Risk Inventory, M204	
1395	ATF	NIBIN	Test Rig Test Evaluation Summary - Phase 1 & 2	Jan 2006
1396	ATF	NIBIN	Test Rig Test Evaluation Summary - Phase 3	Mar 2006
1397	ATF	NIBIN	Testing on Test Rig Test Plan - Phases 1 & 2, NIBIN	Jan 2006

Item ID Number	Component	System or Project	Title	Date
1398	ATF	NIBIN	Testing on Test Rig Test Plan - Phase 3, NIBIN	Mar 2006
1399	JMD	UFMS	Privacy Impact Assessment, UFMS, Working Draft	Dec 2006
1400	DEA	EPIC	EIS Information System Objective Architecture (Draft), EPIC	Aug 1991
1401	DEA	EPIC	EIS Objective System Description, EPIC	Sep 1993
1402	DEA	EPIC	Internal Database Migration Project (Work Plan), EPIC	Jun 1997
1403	DEA	EPIC	Internal Database Migration Requirements, EPIC	Jun 1997
1404	DEA	EPIC	Seizure System Risk Assessment Report, EPIC	May 2005
1405	DEA	EPIC	Information Systems Project management Plan, EPIC	Sep 1991
1408	DEA	EPIC	EIS Risk Impacts, EPIC	
1409	DEA	EPIC	Year 2000 Test Plan, EPIC	
1410	DEA	EPIC	Operational Test Report	Jan 1993
1411	DEA	EPIC	Initial Privacy Impact Assessment for EID	
1412	DEA	EPIC	Development Inspection Logs, EPIC	
1413	ATF	NIBIN	Deployment of the NIBIN Enterprise - Set 9	Jan 2006
1414	ATF	NIBIN	NIBIN Deployment Plan, IBIS 3.4.6 Upgrade	Mar 2006
1415	ATF	NIBIN	NIBIN Deployment Schedule, IBIS 3.4.6	
1416	ATF	NIBIN	Brass TRAX Installation Schedule Template	
1417	JMD	UFMS	Debrief on Vendor Market Analysis Results	Nov 2002
1418	JMD	UFMS	Financial Vendor Response Summary Draft	
1419	JMD	UFMS	Summary of Market Research	
1420	DEA	M204	ST & E Plans and Procedures, Appendix E , Model 204 Corporate Systems	Nov 2004
1421	DEA	M204	Certification Results, Appendix F, Model 204 Corporate Systems	Nov 2004
1422	DEA	Merlin	User Training Plan (Section 1.14 of Proposal 5209)	Dec 2005
1423	DEA	Merlin	Classified Network Integration Test Plan & Procedures	Jun 2006
1424	DEA	Merlin	Merlin Functional Test Plan and Procedures	Jul 2006
1425	DEA	Merlin	Merlin Integration Test Plan and Procedures	Jul 2006
1426	DEA	Merlin	QA Procedures for Merlin Builds	May 2006
1427	DEA	Merlin	Change Management Recommendations	Jun 2006
1428	DEA	Merlin	Requirements for Classified Network Integration Test Facility	May 2006
1429	DEA	Merlin	System Engineering, Infrastructure Test, and Integration (Section 1.2 of Proposal 5209)	Dec 2005
1430	DEA	Merlin	Deployment of the Merlin System Plan (Section 1.1.6 of Proposal 5209)	Dec 2005
1431	DEA	Merlin	Configuration Management Plan for the Merlin Project	Sep 2006
1432	DEA	Merlin	Merlin Quality Assurance Plan	Feb 2005
1433	DEA	Merlin	Merlin Site Checklist	Apr 2007
1434	FBI	Sentinel	Sentinel Phase 1 Privacy Impact Assessment	Feb 2006

APPENDIX VI

SYSTEM SUMMARIES

The system summaries in this appendix contain information from documents the components submitted that we did not verify. The purpose is to provide readers additional information on each system or project and the environment in which it operates or is expected to operate.

The lists of studies, plans, and evaluations include documents representing entire studies, plans, and evaluations we determined complied with one or more of the standards described in Finding 1. The lists do not include all other artifacts the components submitted that we determined contributed to compliance with the standards, such as spreadsheets and briefing slides.

The document titles in the lists may include additional acronyms that we have defined in the text preceding the document list for each system. Acronyms not found in the text of this appendix are located in Appendix II. Blank cells in the Date column indicate items for which no date was provided.

National Integrated Ballistics Information Network
Bureau of Alcohol, Tobacco, Firearms, and Explosives

The ATF's National Integrated Ballistics Information Network (NIBIN) program supports criminal investigations in conjunction with the Integrated Ballistics Identification System (IBIS), a nationally distributed ballistic evidence-imaging database. This database assists state and local law enforcement officials in identification of firearms and bullets collected at crime locations and allows for comparison and correlation to other crime scene evidence or recovered crime guns. NIBIN allows for the ATF to provide ballistic imaging, comparison equipment, and the network over which it communicates to 182 state and local law enforcement partners at 239 data remote sites. State and local NIBIN partners enter bullet and cartridge casing evidence into the systems and conduct electronic comparisons to find potential matches. "Hits" or matches between crimes, not otherwise known to be related, assist law enforcement officials in locating repeat violent offenders. The program began spending funds in FY 1996, and the system is operational.

NIBIN Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007	May 2006	8
Privacy Impact Assessment	Privacy Threshold Analysis, IBIS		9
Risk Management Plan	Risk Assessment, NIBIN and IBIS	Jun 2005	13
Acquisition Plan	Request for Justification for Other Than Full and Open Competition	Jan 2002	12
Security Plan	Security Plan, NIBIN and IBIS	Jun 2005	14
Test Plan	Security Test and Evaluation, NIBIN	Dec 2005	15
Test Plan	Testing on Test Rig Test Plan – Phase 3, NIBIN	Mar 2006	1398
Test Plan	Testing on Test Rig Test Plan – Phases 1 & 2, NIBIN	Jan 2006	1397
Implementation Plan	Deployment of the NIBIN Enterprise – Set 9	Jan 2006	1413
Implementation Plan	NIBIN Deployment Plan, IBIS 3.4.6 Upgrade	Mar 2006	1414
Training Plan	NIBIN Training Set 11, Version 1.2, Draft		17
Contingency/Continuity Plan	Contingency Plan – Appendix I, NIBIN		2
Contingency/Continuity Plan	Contingency Plan, DOJ, NIBIN and IBIS	Jun 2005	3
Test Report	Security Test and Evaluation, NIBIN	Dec 2005	15
Test Report	Security Testing and Evaluation, NIBIN	Dec 2005	16
Test Report	Test Rig Test Evaluation Summary – Phase 1 & 2	Jan 2006	1395
Test Report	Test Rig Test Evaluation Summary – Phase 3	Mar 2006	1396

Inmate Telephone System-II
Bureau of Prisons

The BOP's Inmate Telephone System-II (ITS-II) project began spending funds in FY 1998. The project is a centralized inmate calling system intended to provide inmates with a secure, efficient, and cost effective means of maintaining contact with family, friends, and the community while at the same time preventing crime, fraud, and abuse by inmates. It provides the BOP with enhanced call monitoring, call recording, and reporting capabilities. ITS-II is funded and maintained using non-appropriated funds generated from the Commissary Trust Fund. Maintenance costs for the system are established and funded from the actual costs of service charges for telephone usage. Annual funding is based on the projected sales for that year which exceeds the outlays for the project. ITS-II is fully installed and is in a steady-state status. It consists of local networks at all BOP facilities and primary and secondary Central Office Facilities and is connected via a Wide Area Network.

ITS-II Studies, Plans, and Evaluations

Document Type	***Title***	***Date***	***Item #***
Market/Other Research	Request for Comment		416
Business Case Study	Analysis of Alternatives, Next Generation Inmate Telephone System	Jul 1996	18
Business Case Study	OMB Exhibit 300 BY 2006		1392
Privacy Impact Assessment	Privacy Impact Assessment	Apr 2006	20
Acquisition Plan	Individual Acquisition Planning	Jan 1997	19
Project Plan	Program Plan	May 2005	412
Security Plan	Inmate Telephone System (ITS-II) Security Plan	Dec 2004	21
Systems Engineering Management Plan	Engineering Management Plan	Apr 2005	415
Conversion Plan	Site Network Integration Plan, ITS-II/TRUFACS	Nov 2001	22
Implementation Plan	Site Network Integration Plan, ITS-II/TRUFACS	Nov 2001	22
Contingency/Continuity Plan	Contingency Plan	Nov 2004	414

Concorde
Drug Enforcement Agency

The DEA is the federal entity charged with the enforcement of the controlled substance laws and regulations. It has approximately 300 locations throughout the world and utilizes various "stove-piped" applications in support of primary businesses – criminal data gathering, case status tracking, lab analysis, evidence and seized asset handling, licit drug manufacturing and distribution tracking (DEA's diversion function), and administrative functions such as tracking agent property (weapons, fleet, badges), and agent tasking. The Concorde program is intended to eliminate these stove-piped systems by integrating business functions and allowing for information sharing across the main DEA business areas.

Concorde Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Privacy Impact Assessment	Initial Privacy Impact Assessment , Concorde		35
Risk Management Plan	Risk Management Plan, Concorde, Version 1.0	Feb 2005	46
Acquisition Plan	Statement of Work/Acquisition Plan, Concorde, Version 1.0	Nov 2002	49
Project Plan	Project Management (PMP), IMPACT Fiscal Year 2004, Version 2.1	Sep 2004	42
Project Plan	OMB Exhibit 300 for BY 2007	Sep 2005	39
Security Plan	System Security Authorization Agreement (SSAA), Appendix E, Web Architecture	Mar 2002	50
Configuration Management Plan	Configuration Management Plan, Concorde, Version 1.0	Jul 2004	29
Quality Assurance Plan	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005	83
Test Plan	Project Test Plan (PTP), IMPACT, Release 2.0, Version 1.0	Feb 2005	44
Implementation Plan	Project Deployment Plan, Concorde, Version 1.0	Sep 2004	41
Training Plan	Training Program, PMP Concorde, FY 2006, Version 1.0	Oct 2005	51
Contingency/Continuity Plan	Contingency Plan, Web Architecture, Version 2.0	Mar 2006	30
Test Report	Operational Test for Impact on Security (OTIS) Report of the Pilot Implementation, IMPACT	Jul 2002	40
Test Report	System Security Authorization Agreement (SSAA), Appendix E, Web Architecture	Mar 2002	50
Performance Evaluation	OCIO: Project Dashboard Project Managers Worksheet, Concorde	Aug 2005	38

In the 1990's, DEA introduced the agency-wide Firebird client/server, which is the core local area network. Concorde is built on the Firebird infrastructure. The focus of Concorde is the investigative and case management process.

The Concorde project is composed of four major technology enhancements: Investigative Management Program and Case Tracking System (IMPACT), Plan Enforcement Tracking System (PlanETS), Statistical Management and Report Tracking System (SMARTS), and the Centralized Evidence Reporting and Tracking System (CERTS). Although the OMB exhibit 300 shows the project began spending funds in FY 2003, IMPACT's pilot implementation was released in 1999. The scheduled completion for the entire project is the end of FY 2009.

E-Commerce
Drug Enforcement Agency

The DEA's Office of Diversion Control (OD) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and to ensure that there is a sufficient supply for legitimate medical uses while preventing the introduction of contraband controlled substances into the legal distribution channels.

E-Commerce Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	Economic Impact Analysis of the Electronic Orders Rule	Mar 2005	58
Business Case Study	Initial Economic Impact Analysis of the Proposed Electronic Orders Rule	Mar 2003	61
Business Case Study	OMB Exhibit 300 for BY 2007, Final CSOS	Sep 2005	64
Privacy Impact Assessment	Detailed Privacy Impact Assessment, Attachment: DEA CSOS Privacy Policy, Section IV	Sep 2005	56
Risk Management Plan	Facilitated Risk Assessment Process, DEA Diversion Control E-Commerce PKI, SSAA, Appendix G, Version 1.0	Dec 2003	60
Risk Management Plan	Risk Management Plan, DEA Diversion Control, E-Commerce System, Version 1.0	Oct 2005	72
Project Plan	Program Management Plan, DEA Diversion Control E-Commerce PKI, Version 3.1	Nov 2004	68
Security Plan	System Security Plan, CSOS, Version 1.0	Jun 2005	74
Systems Engineering Management Plan	Operational and Technical Architecture, Public Key Infrastructure Analysis, DEA Diversion Control E-Commerce PKI	Jun 2003	65
Configuration Management Plan	Configuration Management Plan, DEA Diversion Control E-Commerce System, Version 1.0	Feb 2006	53
Quality Assurance Plan	Process and Product Quality Assurance, DEA Diversion Control E-Commerce System, Version 1.0	May 2005	67
Test Plan	Acceptance Test Plan, Public Key Infrastructure Analysis, Diversion PKI, CSOS	Jan 2005	52
Test Plan	Test Plan and Reporting Procedures, CSOS/ EPCS	Dec 2001	75
Training Plan	Training Plan, Public Key Infrastructure Analysis, DEA Electronic Commerce PKI	Aug 2002	76
Contingency/Continuity Plan	Contingency Plan, DEA Diversion Control E-Commerce PKI System (EPCS/CSOS), Version 1.0	Nov 2003	54

Document Type	*Title*	*Date*	*Item #*
Contingency/Continuity Plan	Contingency Plan, DEA Diversion E-Commerce System Security Plan, Appendix L, Version 1.1	May 2005	55
Test Report	System Security Authorization Agreement (SSAA), Appendix F, CSOS and EPCS PKI	Mar 2004	73
Post-Implementation Evaluation	Diversion Metrics Implementation Report, DEA Diversion Control, E-Commerce System, Version 1.0	Jan 2006	57

The Government Paperwork Elimination Act (GPEA) of 1999 (Title XXII of Public Law 105-277) mandates that Federal agencies allow for the option of electronic submission of required records and for the use of electronic signatures when practicable.

In July 1999, DEA undertook the initiative to begin designing two e-commerce initiatives that would enable industry to conduct e-commerce. The first project was called the Manufacturers and Distributors (MADI) Public Key Infrastructure (PKI) Analysis and Design Program, which involved the designing of a PKI proof-of-concept to better oversee and manage the transfer of Schedule II controlled substances between DEA registrants, manufacturers, wholesalers, and pharmacies. The second project was called DEA – Department of Veterans Affairs (DEVA) PKI Pilot Program, which involved designing a public key infrastructure architecture suitable for use in transmitting prescriptions electronically and identifying aspects of the relationship between the physician and the pharmacy that can be enhanced through the implementation of a PKI.

The initial phases of both projects entailed requirements and design analysis. The next phases of the e-commerce projects introduced a change in the project titles: Controlled Substance Ordering System (CSOS) and Electronic Prescriptions for Controlled Substances (EPCS). The DEA and DVA pilot continues under the EPCS project.

The CSOS/EPCS project began spending funds in FY 1999 and is estimated to be complete in FY 2016. The DEA has begun the collection and analysis of CSOS orders.

El Paso Intelligence Center (EPIC) Information Systems
Drug Enforcement Agency

Other Components Involved: Federal Bureau of Investigation
U.S. Marshals Service
Bureau of Prisons

EIS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	National Drug Seizure System Discussion Paper, CDX	Feb 2004	432
Market/Other Research	NDSS Project, Background: NIBRS/UCR Data, CDX	May 2003	427
Business Case Study	OMB Exhibit 300 for BY 2007	Sep 2005	77
Privacy Impact Assessment	Initial Privacy Impact Assessment for EID		1411
Risk Management Plan	EIS Risk Impacts, EPIC		1408
Risk Management Plan	Risk Assessment Report, EPIC	May 2005	417
Risk Management Plan	Risk Management Plan, Open Connectivity Project, DEA EPIC, Revised	Aug 2004	429
Risk Management Plan	Seizure System Risk Assessment Report, EPIC	May 2005	1404
Project Plan	Information Systems Project management Plan, EPIC	Sep 1991	1405
Security Plan	System Security Plan, ESS	Aug 2005	420
Systems Engineering Management Plan	System Engineering Management Plan, EPIC Open Connectivity Project	Jun 2004	424
Configuration Management Plan	Configuration Control Board (CCB) Charter and Request for Information Technology Services (RITS) Policy	Feb 2004	425
Quality Assurance Plan	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005	83
Verification/Validation Plan	Verification and Validation Plan, EPIC Open Connectivity Project	Apr 2004	426
Test Plan	Development Inspection Logs, EPIC		1412
Test Plan	Year 2000 Test Plan, EPIC		1409
Training Plan	Training Plan, EPIC Open Connectivity Project	Jun 2004	423
Contingency/Continuity Plan	Contingency Plan, ESS	Mar 2006	422
Test Report	Development Inspection Logs, EPIC		1412
Test Report	Operational Test Report	Jan 1993	1410

EPIC accomplishes its mission in part by manually processing written or telephonic requests for information received from State, local and Federal law enforcement personnel, on persons, modes of transportation, organizations, or addresses that are suspected of being engaged

in, or associated with some criminal activity. Watch Officers using a multiple database query process the requests for information.

The objective of the Open Connectivity Project is to enable EPIC to provide secure internet access to tactical intelligence information for Federal, State and Local law enforcement agencies. The system objective is to streamline access by providing to all EPIC customers a point of entry that permits direct and remote electronic access from the users' existing IT and internet architecture and provides an automated response to queries. With the Open Connectivity Project, EPIC will provide this access for its customers in the form of a secure, Internet connection. Through an EPIC web site, law enforcement officers will access EPIC services, which will include the multiple source data repository, comprehensive query results, multiple formatted reports, and automated analytical support.

Firebird
Drug Enforcement Agency

Firebird is the DEA's global computing infrastructure, providing the foundation for the communications network, the client and server hardware and software, and the DEA's complete office automation system to all DEA personnel and contractors. A client-server based network, Firebird links DEA offices and components worldwide and supports the full spectrum of DEA operations. Firebird enables the DEA's investigative case management system, the financial management system, and all other Sensitive But Unclassified (SBU) information systems that DEA personnel use to support their daily job functions. Firebird also provides the interface for all new web-based applications and lays the foundation for improved information sharing with partner agencies.

Firebird Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Firebird Information Technology Support (FITS) Market Research Report	Mar 2004	1379
Business Case Study	OMB Exhibit 300 for BY 07	Sep 2005	1378
Project Plan	Project Management Plan (PMP), Firebird Infrastructure Technology Services (FITS), Version 3.0	Jan 2006	129
Security Plan	Security Operating Procedures Guide, Firebird (FSOPG), Version 4.0	Mar 2004	1021
Configuration Management Plan	Configuration Management Plan (CMP), FITS, Version 1.3	Jan 2006	116
Quality Assurance Plan	Quality Assurance Plan, FITS, Version 2.1	Jan 2005	130
Test Plan	Security Test and Evaluation Plan and Procedures, Appendix E	Jul 2004	131
Implementation Plan	EOS Software Deployment Function Description, Version 2.5, not dated		118
Implementation Plan	Windows 2003 (W2K3) Implementation Plan, FITS MDE, Version 1.2	Jun 2006	139
Contingency/Continuity Plan	Windows Server 2003 Infrastructure Disaster Recovery Document, FITS, Version 2.1	Jun 2006	141
Test Report	Test Matrix, Desktop and Server Management Evaluation 2005		137
Performance Evaluation	Enterprise Health and Performance Metrics Review	May 2006	117
Performance Evaluation	Firebird Dashboard	Apr 2006	121
Performance Evaluation	SIO Firebird project portfolio	Jul 2006	132

In 1994 the DEA began replacing its proprietary Wang Office Automation (OA) system with Firebird. The OA system provided personnel with basic office automation software and access to DOJ mainframe systems, but did not allow for electronic case management, or electronic communications and information sharing between DEA offices. The DEA designed Firebird based on forward looking enterprise-wide and Federal IT standards, the recognized advantages of a modular architecture, and the need for a flexible system that is maintainable and expandable.

The Firebird project began spending funds in FY 1994, and entered the Operational/Maintenance phase in FY 2003. In May 2003, the DEA completed its initial deployment of Firebird, which supports nearly 16,000 users, over 14,500 workstations, and over 500 servers in more than 370 locations worldwide.

Model 204 Corporate Systems
Drug Enforcement Agency

Other Components Involved: Federal Bureau of Investigation

The DEA performs mainframe data processing activities utilizing Computer Corporation of America (CCA) Model 204 database management system software for the development of applications for the corporate mission and administrative databases. These Model 204 Corporate Systems applications or subsystems provide the capability for DEA personnel to acquire information relating to drug related activities and cases. The applications also provide a method to track administrative information relating to DEA equipment and personnel.

M204 Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007	Jul 2005	80
Project Plan	Project Management Plan (PMP), Events Activity Subsystem (EVENTS), Calendar Year 2004, Version 1.0	Jun 2004	82
Security Plan	Systems Security Authorization Agreement (SSAA), Model 204 Corporate Systems (M204)	Nov 2004	85
Configuration Management Plan	Project Level Configuration Management Plan, Events Activity Subsystem (EVENTS), Version 1.0	Jun 2004	81
Quality Assurance Plan	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005	83
Verification/Validation Plan	Independent Verification and Validation (IV&V) Software Testing Procedure for Mainframe Environment, Version 2.0	Jun 2004	79
Test Plan	ST & E Plans and Procedures, Appendix E, Model 204 Corporate Systems		1420
Test Report	Certification Results, Appendix F, Model 204 Corporate Systems		1421

The M204 system includes approximately 32 core investigative and administrative applications that support DEA's mission, strategic goals, and objectives as well as serving the specific needs of external DEA partners. Several of the legacy applications now running in the M204 environment are scheduled for replacement through a number of modernization initiatives. To enhance the usability and simplify access to M204 applications until the modernization initiatives deploy viable solutions, DEA has acquired and is implementing JANUS Web Server to provide browser based access to selected M204 applications. JANUS will replace the mainframe "green screen" with user friendly drop down menus, data entry validation and navigation features.

The M204 project began spending funds in FY 1980, and is in the operational/maintenance phase of the DEA SDLC.

Merlin
Drug Enforcement Agency

Merlin provides DEA offices with the capability to transmit, access, and share classified intelligence data over the existing classified telecommunications networks that service the DEA's domestic and foreign offices.

The Merlin system provides the end-users workstations and the necessary enterprise and site-level servers to run Active Directory services, mail services, local file services, and a Merlin Web site. The Merlin system provides the end users with a complement of commercial applications such as Microsoft Office, i2's Analyst's Notebook, and ArcView. It also provides the users access to DEA custom applications that use a browser (Internet Explorer) interface.

Merlin Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007		271
Risk Management Plan	Risk Assessment Report, DEA Classified Infrastructure Support System	May 2005	261
Project Plan	Merlin Program Plan, Version 2	Jun 2006	268
Security Plan	System Security Authorization Agreement (SSAA), DCISS	Aug 2003	272
Configuration Management Plan	Configuration Management Plan for the Merlin Project	Sep 2006	1431
Quality Assurance Plan	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005	83
Quality Assurance Plan	Merlin Quality Assurance Plan	Feb 2005	1432
Test Plan	Security Test & Evaluation Plan and Procedures	Aug 2003	1384
Contingency/Continuity Plan	Contingency Plan for the DEA Merlin Program	Jun 2006	259
Test Report	Certification Results	Aug 2003	1385
Test Report	COOP Test Report using VERITAS Replication EXEC 3.1	Mar 2006	260
Test Report	System Security Authorization Agreement (SSAA), DCISS	Aug 2003	272
Performance Evaluation	Earned Value Management (EVM) Merlin, Doc #12-35-41-55	Jul 2006	262
Performance Evaluation	Merlin Dashboard - May	Jun 2006	264

Organized Crime Drug Enforcement Task Force Fusion Center System
Office of the Deputy Attorney General

Other Components Involved: Executive Office for the U.S. Attorneys
Bureau of Alcohol, Tobacco, Firearms, and Explosives
U.S. Marshals Service
Federal Bureau of Investigation
Criminal Division
Tax Division

The mission of the OCDETF Fusion Center (OFC) is to fuse data from multiple disparate sources and extract previously unidentified relationships and knowledge from the fused data relating to persons and organizations. The OFC will support the OCDETF intelligence and investigative activities task force with a fused database comprised of information from its member agencies. The Fusion Center System is a web based application that will be used by the OFC analysts and agents to search on information contained within this fused database. OCDETF began spending funds on the Fusion center system in FY 2003.

OFC Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Comparative Analysis of the FBIs SCOPE and DEAs NEDRS Systems	Feb 2003	1377
Market/Other Research	Comparative Analysis of the FBI's SCOPE and FTTTF	Apr 2003	1372
Market/Other Research	Draft Comparative Analysis of OCDETF Requirements with Existing DOJ Data Warehousing Efforts	Apr 2003	1371
Market/Other Research	Third Party Tool Recommendations	Jun 2005	1369
Business Case Study	OMB Exhibit 300 for BY 2006	Sep 2004	316
Privacy Impact Assessment	Privacy Impact Assessment, OFC (Draft)	Aug 2004	320
Risk Management Plan	Risk and Issue Management Master Plan	Jun 2005	328
Acquisition Plan	Justification for Other than Full and Open Competition	May 2004	306
Project Plan	Project Management Plan, OFC Deployment	Sep 2005	321
Project Plan	Project Plan, Software Version 1.0, OFC	May 2006	322
Security Plan	System Security Plan, OFC Compass		334
Quality Assurance Plan	Quality Management Plan (QMP), Office of Information Systems (SI), Version 4.1	Sep 2005	83
Test Plan	System Test Plan, OFC, Version 1.2	Jan 2006	335
Training Plan	Compass Training Plan, OFC, Version 1.0	Sep 2005	289
Contingency/Continuity Plan	IT Contingency Plan, IRSS, Version 2.2	Mar 2005	305
Test Report	System Test Plan, OFC, Version 1.2	Jan 2006	335

eWorld
Executive Office for Immigration Review

The Executive Office for Immigration Review's (EOIR) eWorld project began spending funds in FY 2002 and is the agency's primary initiative in its capital planning and investment control process. In this multi-year, multi-phased, multi-disciplinary project, EOIR will make the transition from paper to electronic documents for its official adjudication records spanning from initial filing through final appellate decisions.

eWorld Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Market Survey, EOIR, Digital Audio Recording Project, Version 0.16 (Draft)	Apr 2006	854
Business Case Study	OMB Exhibit 300 for BY 2007	Jan 2006	112
Privacy Impact Assessment	Privacy Impact Assessment, Executive Office for Immigration Review	Apr 2006	860
Project Plan	Project Management Plan, CASE Court Pilot	Apr 2006	851
Project Plan	Project Management Plan, Digital Audio Recording Project, Version 0.05	May 2006	852
Security Plan	System Security Plan (SSP) for JCON-II/CASE, EOIR	Mar 2006	863
Configuration Management Plan	Configuration Management Plan, EOIR	Mar 2006	856
Configuration Management Plan	Configuration Management Plan, eWorld, Version 1.0 (Draft)	Feb 2006	857
Contingency/Continuity Plan	IT Contingency Plan, EOIR, JCON-II/CASE, Version 2.0	Nov 2005	855

Biometric Reciprocal Identification Gateway
Federal Bureau of Investigation

The FBI's IAFIS is a 10-rolled fingerprint identification system that is used by federal, state, and local law enforcement and authorized non-criminal justice agencies to identify subjects with criminal histories. The DHS IDENT is a 2-flat fingerprint identification system originally deployed by the Immigration and Naturalization Service as a database of criminal and illegal aliens to assist Border Patrol in identifying aliens who repeatedly attempt illegal border crossings. The DHS utilizes IDENT for search and enrollment purposes when non-US citizens travel to the United States through an authorized port of entry. The Department of State (DOS) Consular Posts utilize IDENT for search and enrollment purposes when determining suitability for aliens traveling to the United States. Currently, IAFIS and IDENT are linked through limited automated and manual processes.

BRIDG Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	Full Business Case, IDENT-IAFIS Interoperability, iDSM Project	Jan 2006	455
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1036
Privacy Impact Assessment	Privacy Impact Assessment for the DOJ/FBI-DHS Interim Data Sharing Model (iDSM)		459
Risk Management Plan	Risk Management Plan, iDSM Project	Jan 2006	462

The FBI supports DHS and DOS through daily biographic-based extracts of wants and warrants that have an associated FBI number and Known and Suspected Terrorists. The extract process, however, does not provide real-time access to current information, includes only a subset of information, and does not allow international, federal, state, and local fingerprint contributors access to all immigration information. Various legislative acts demand that the FBI and DHS ensure that the biometric systems are able to seamlessly share data that is complete, accurate, current, and timely. Through this interoperability, the criminal and immigration information will be accessible to and shared among other federal, state, and local law enforcement agencies.

In order to realize interoperability, investment is needed to develop the Biometric Reciprocal Identification Gateway (BRIDG). BRIDG development is planned in three phases: interim Data Sharing Model (iDSM); Initial Operating Capacity (IOC); and the Full Operating Capacity (FOC). In FY 2008, investment is needed to support the operation and maintenance of the iDSM and development of both the IOC and FOC portions of the BRIDG. The BRIDG investment will allow the creation and maintenance of biometric-based links between the biographic information contained in the IAFIS and IDENT systems, in near real time, as well as provide the infrastructure necessary to exchange data between the systems to ensure that biometric-based immigration and travel history information and criminal history record information is available to authorized personnel.

Computer Analysis Response Team Storage Area Network
Federal Bureau of Investigation

In the aftermath of the September 11, 2001 terrorist attacks, the FBI collected digital evidence from businesses, personal computers and loose media from across the US. The FBI did not possess a storage/examination/review system that could efficiently and consistently process large quantities of digital evidence collected from multiple sources. The Computer Analysis Response Team Storage Area Network (CARTSAN) System is a unique state-of-the-art "Digital Forensic Network" that allows for the efficient forensic processing and review of computer evidence. This system was certified and accredited on August 15, 2005. It offers the Computer Analysis Response Team (CART) Examiner and FBI Case Agent a resource that ensures accurate and timely handling of computer evidence acquired in support of Criminal, Cyber, Counterintelligence and Counterterrorism matters in a forensically secure environment.

CARTSAN Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1023
Privacy Impact Assessment	Privacy Impact Assessment, CARTSAN, (Draft)		446
Risk Management Plan	Risk Management Plan	Jul 2005	447
Security Plan	System Security Plan, CARTSAN	Aug 2005	449
Configuration Management Plan	Configuration Management Plan, Version 0.1 (Draft)		438
Quality Assurance Plan	Digital Evidence Laboratory Quality Assurance Manual Supplement, CART	Apr 2006	439
Test Plan	Certification Test Report, CARTSAN	Aug 2005	436
Implementation Plan	CARTSAN Review Network Installation Plan	Jun 2005	434
Test Report	Certification Test Report, CARTSAN	Aug 2005	436
Performance Evaluation	Earned Value Management Worksheet	Jul 2005	441
Performance Evaluation	Investment Management/Project Review Board	Aug 2005	443

Each CARTSAN System has the ability to temporarily store large quantities of digital computer evidence. This system establishes digital connectivity between the CART forensic examination and review processes, eliminating the need to store forensic examination data on multiple hard drives. The system greatly reduces the time required to process and disseminate computer related evidence.

In FY 2006, CART anticipates completing more than 10,000 examinations of computer media, equating to more than one Petabyte of digital evidence. One Petabyte of information is equivalent to 250 billion pages of text; enough to fill 20 million, four-drawer filing cabinets. As the amount of data average businesses collect and store is doubling each year, this amount of data will be what many businesses will be managing within the next 5 years. As this growth

occurs, the FBI is required to expand its capability to process and temporarily store these increasing amounts of data.

Phase I of the CARTSAN project, initiated in FY 2002 and concluded in FY 2006, included the design, acquisition, and deployment of CARTSAN Systems to 25 major FBI Field Office and Regional Computer Forensic Laboratories (RCFL) locations. Phase II is scheduled to begin in BY 2007 with the allocation of personnel resources to begin planning for the next deployment of systems. Phase II includes the purchase and deployment of 20 new CARTSAN Systems as well as operation, maintenance and upgrade costs for the existing 25 systems.

Combined DNA Index System
Federal Bureau of Investigation

The Combined DNA Index System (CODIS) is an automated DNA information processing and telecommunications system that supports the National DNA Index System, State DNA Index System, and Local DNA Index System. The concept behind CODIS is to create a database of the States' convicted offender profiles to help solve violent crimes for which there are no suspects. CODIS enables Federal, State, and local forensic laboratories to exchange and compare DNA profiles electronically, thereby linking serial violent crimes to each other and to known offenders. CODIS uses two indexes to generate investigative leads in crimes where biological evidence is recovered from the crime scene. The Convicted Offender Index contains profiles of individuals convicted of felony offenses and other crimes. The Forensic Index contains DNA profiles developed from crime scene evidence, such as semen stains or blood.

This investment began in 1990 and is scheduled to be completed by January 2010.

CODIS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	FY 2008 Full Business Case	Dec 2005	467
Privacy Impact Assessment	Privacy Impact Assessment, National DNA Index System (NDIS) Database	Oct 2004	471
Risk Management Plan	Risk Management Plan, CODIS, Draft Version 01	May 2006	473
Acquisition Plan	Single Acquisition Management Plan for the Combined DNA Index System	Feb 2006	475
Project Plan	Product Management Plan, CODIS Bridge Contract Extension	Sep 2005	472
Security Plan	System Security Plan, CODIS	Jan 2005	476
Contingency/Continuity Plan	Three Part Contingency Plan, CODIS Bridge Contract Extension	Oct 2005	477

Data Centers Unit
Federal Bureau of Investigation

The Data Centers project began spending funds in FY 2004. The project consists of: (1) operations and maintenance of installed computing platforms, data storage devices, and a channel extension network; (2) modernization of computing platforms, operating systems, data storage devices, and channel extension; (3) enhancement of existing hardware / software (for example, for storage expansion, greater processing capacity, process improvement, and systems integration); and (4) periodic development for new technology or projects such as robotic tape libraries and channel extension (past) and an enterprise backup solution (future). The mission of the Data Centers Unit is to provide an IT infrastructure and effective, efficient, and timely technical support that is the foundation for supporting the FBI's priorities. The major goal of the Data Center Unit is to provide continuous, effective automated production workload support and business continuity for all FBI investigative and administrative missions.

DCU Studies, Plans, and Evaluations

Document Type	***Title***	***Date***	***Item #***
Business Case Study	OMB Exhibit 300 for BY 2008	Jul 2005	489
Project Plan	Contribution of the Mainframe to the Bureau's Mission, FBI	Feb 2006	481
Project Plan	Project Plan, Global Mirroring Project	Dec 2005	490
Security Plan	System Security Plan, FBI, Enterprise Servers, Version 1.2	Oct 2004	492
Contingency/Continuity Plan	Continuity of Operations Plan, FBI, ITOD, Operations Section	Jan 2005	480
Performance Evaluation	Project Summary Report, ITOD Mainframe System Upgrade		491

Digital Collection System
Federal Bureau of Investigation

The Digital Collection project began spending funds in FY 1997. Digital Collection consists of the DCS-3000, DCS-5000, and DCS-6000, which provide digital collection tools, foreign counterintelligence gathering, and law enforcement evidence collection, respectively.

DCS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1024
Privacy Impact Assessment	Privacy Impact Assessment, SPIDERNET and DIGITAL STORM	Aug 2001	510
Privacy Impact Assessment	Privacy Impact Assessment, Upgrade from SPIDERNET to Red Wolf	Dec 2005	511
Risk Management Plan	Risk Assessment and Management Plan (RAMP), DCS-6000, Systems Security Plan, Appendix L, Version 2.0	May 2006	521
Project Plan	Project Plan, Digital Collection System, Digital Collection - 05	Nov 2004	516
Project Plan	Project Plan, Digital Collection, Digital Collection - 03	Aug 2003	517
Project Plan	Project Plan, Digital Collection, Digital Collection - 04	Jan 2004	518
Project Plan	Project Plan, Digital Storm	Jun 1998	519
Security Plan	System Security Plan, DCS 3000, Version 2.0	Apr 2006	524
Security Plan	System Security Plan, DCS-5000, Revision 3.5	Dec 2005	525
Security Plan	System Security Plan, DCS6000 Voice Box III, Version 3.1	May 2006	526
Test Plan	Test Plan, Digital Storm, Version 1.0	Feb 1999	527
Performance Evaluation	Project Status Report, DCS-5000	Jun 2006	520
Post-Implementation Evaluation	Phase Review Report, Phase 1/2, Project Digital Storm,	Aug 1998	509
Post-Implementation Evaluation	Project Closeout Report, Digital Collection - 04, Version 1.1	Jul 2005	514

Today's information technology capabilities afford terrorists and criminals many avenues to coordinate and commit offenses against US citizens and interests. Traditional phones were the primary avenue criminals used to communicate information regarding unlawful acts. Today, more incidents are committed and facilitated by terrorists using high-tech, non traditional communications methods. Communications methods are dramatically increasing in number and complexities, resulting in the continual and evolving need for advanced methods of electronic surveillance of voice communications - methods of electronic surveillance have limited-life utility in intercepting newer, more secure types of publicly offered communications.

The expansion of electronic surveillance activity in frequency, sophistication, and linguistic needs continues to increase the level of support required. An important factor behind this expansion is the changing demographic of targets that must be monitored by investigators. The FBI must supply equipment and analytical tools to uniquely qualified language specialists to speed the translation and transcription process to meet the investigators' needs. Further, the life span of today's technology is often much shorter than older technologies, resulting in more frequent need for solution development. Terrorist and criminal activity has expanded across international boundaries. Current United States-based intercept technologies and collection capabilities are not always sufficient to meet global requirements. Increased coordination and cooperation with other government agencies and governments of other countries place are needed.

Digital collection must continue to clearly define electronic surveillance requirements and closely track manufacturers' approaches and solutions. Collection equipment manufacturers continue toward complying with technical standards as a result of the Communications Assistance to Law Enforcement Act (CALEA). One result of the CALEA standard is more information is available for collection. This increase in data coupled with the increased complexity of computer-based electronic surveillance information management systems will impose a requirement for efficient distribution to users and their respective collection systems.

Electronic Surveillance Data Management System
Federal Bureau of Investigation

The Electronic Surveillance (ELSUR) Data Management System (EDMS) project began spending funds in FY 2004. The system ensures the timely and proactive collaboration, analysis, and integration of Title III and Foreign Intelligence Surveillance Act (FISA) intelligence and evidence collected from lawfully authorized digital intercepts and seizures.

EDMS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007	Sep 2005	540
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1025
Privacy Impact Assessment	Privacy Impact Assessment (PIA), Draft	Sep 2005	529
Risk Management Plan	Risk Management Plan, EDMS	Aug 2000	547
Risk Management Plan	Risk Management Plan, EDMS, Version 3.0		548
Project Plan	Project Plan, Project EDMS (ELSUR Data Management System)	Feb 2004	544
Security Plan	System Security Plan, EDMS, version EDMS SSP Rev. 2.0	Apr 2004	553
Configuration Management Plan	Configuration Management Plan, Revision b	Sep 2005	532
Test Plan	Certification Test Plan	Apr 2004	531
Test Plan	Test and Evaluation Master Plan, EDMS, Revision A	Aug 2005	555
Conversion Plan	Target EA and Transition, EDMS Enterprise Architecture, Executive Summary, Version 1.0	Jan 2005	554
Contingency/Continuity Plan	Continuity of Operations Plan	Apr 2004	533
Performance Evaluation	EDMS Briefing for the FBI Science and Technology Advisory Board	Jul 2005	536
Performance Evaluation	Project Status Report, ELSUR EDMS	Apr 2006	546
Performance Evaluation	Department Investment Review Board		535
Performance Evaluation	Monthly Project Status Reporting		543

EDMS integrates and consolidates ELSUR products, such as wiretaps, telephone, email, and seized media from multiple field collection systems. As ELSUR products are consolidated into EDMS, the system performs multiple functions, including indexing, data minimization (for legal compliance), language translation, data prioritization, and other functions. Most importantly, EDMS provides the capability for agents, translators, and analysts to have increased access to many types of ELSUR data extracted from multiple collection sources to view and

analyze within a single system. This significantly increases the FBI's ability to manage, analyze, and share ELSUR products and greatly improves the efficiency with which investigators can develop leads and intelligence through integrating best-of-breed automated and interoperable data analysis capabilities.

While providing significant tactical value, EDMS cannot continue to support the FBI's counterintelligence and counterterrorism mission objectives as it currently exists due to the increase in data collection volume and user base. Since October 2004, EDMS experienced a 300 percent increase in average users per month. Over the past 3 years, the volume of ELSUR collections has grown over 62 percent for audio wire-taps and over 3,034 percent for digital collections such as email and seized media. The current system is unable to scale and meet these growing demands. Because of the increased burden, the ability to share ELSUR data and collaborate efficiently with other authorized federal, state, local law enforcement and federal intelligence agencies will no longer be feasible unless the proposed enhancements are implemented.

The budget year 2008 primary objectives are to: provide additional disk capacity to support current and anticipated storage needs; enhance current system security controls to adequately protect data; upgrade interfaces and data loaders to provide for increases in data volume inputs and more efficiently manage data; and acquire additional software licenses and processors to accommodate anticipated increase in users.

Foreign Terrorist Tracking Task Force
Federal Bureau of Investigation

In 2001, Homeland Security Presidential Directive-2 established the Foreign Terrorist Tracking Task Force (FTTTF) to provide actionable intelligence to law enforcement to assist in the location and detention and ultimate removal of terrorists and their supporters from the US.

In 2005, a White House Memorandum on Strengthening the Ability of the Department of Justice to Meet Challenges of the Security of the Nation directed the Attorney General to establish a "National Security Service" and to combine the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI under the leadership of a senior FBI official. As a result, the FBI created the National Security Branch. This Branch will enable FBI to meet information sharing Presidential Guidelines and Initiatives such as the Intelligence Reform and Terrorism Prevention Act of 2004.

FTTTF Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1026
Risk Management Plan	Risk Management Plan, Guardian, Version 1.0	Apr 2006	565
Project Plan	Project Management Plan (Software Development Plan), Guardian 2.0, Version 9.0	Mar 2006	564
Systems Engineering Management Plan	System Engineering Management Plan, Guardian, Draft Version 11.0	Mar 2006	567
Test Plan	Test and Evaluation Master Plan, Guardian, Version 1.0	Mar 2006	568
Implementation Plan	Installation Plan, Guardian 2, Draft Version 5.0	Apr 2006	561

In FY 2006, an FBI assessment determined that existing HPSD-2 national security and counterterrorism operations would be enhanced by providing analysis and technology support by capitalizing on FTTTF's existing operations in line with FBI's Enterprise Architecture. This will enable multiple Divisions to consolidate technological and analytical resources to support the combined activities of the counterterrorism, counterintelligence, and intelligence elements of the FBI. As part of this mission, the National Security Branch must deliver new analytical capabilities and operational products (such as activity reports, records, and information), real-time to State, local law enforcement, Tribal, FTTTF, National Counterterrorism Center, and other agencies. This data warehousing for search and retrieval capability will leverage best information and querying practices for information sharing through FBI's architecture and electronic directory services across domains. These technological solutions will increase the efficiency in sharing information with State, local and Tribal law enforcement and make it easier for the FBI to access and analyze the information. This solution supports consolidation of resources to combine activities of the counterterrorism, counterintelligence, and intelligence elements of the FBI.

The FTTTF project began spending funds in FY 2005. This FY 2008 justification is designed to address the core IT strategy of the FTTTF and the National Security Analysis Center

(NSAC) while providing the framework for integration into the National Security Branch's Analytical Capabilities Program. This IT enhancement will support the core strategy of the NSB.

Integrated Automated Fingerprint Identification System
Federal Bureau of Investigation

The Integrated Automated Fingerprint Identification System (IAFIS) is a rapid, electronic fingerprint identification and criminal history system that responds to law enforcement agencies within two hours and to authorized civil agencies within 24 hours. Prior to the IAFIS, fingerprint identification was a manual, labor-intensive process which took weeks or months to complete. The IAFIS provides identification, image exchange, and criminal history services to more than 80,000 law enforcement agencies and qualified civil agencies. The IAFIS is internationally recognized as the biometric system leader and contains the largest fingerprint repository in the world.

IAFIS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1027
Security Plan	Operational System Security Plan, AFIS	Jan 1999	588
Security Plan	System Security Plan, IAFIS, Version 2.1	Mar 2006	591
Systems Engineering Management Plan	Systems Engineering Management Plan, Criminal Justice Information Services Division	Jul 2005	592
Systems Engineering Management Plan	Systems Engineering Management Plan, SoSSS, Revision 2.2 Final	Nov 2005	593
Configuration Management Plan	Configuration Management Plan, Criminal Justice Information Services Division, Revision1.2	Aug 2002	582
Quality Assurance Plan	Quality Assurance Plan, CJIS Division	Mar 2005	589
Verification/Validation Plan	Independent Verification, Validation & Testing (IVV&T) SOW, CJIS Division	Nov 1993	586
Test Plan	Build E System Integration and Test Plan (SITP), IAFIS	Jan 1998	577
Test Plan	IAFIS System Acceptance Test Plan, Volume 1	Feb 1999	584
Conversion Plan	Transition Plan, IAFIS, Second Iteration	Apr 1998	596
Conversion Plan	Transition Plan, IAFIS, Third Iteration	Oct 1998	597
Implementation Plan	Build D Installation Plan	Nov 1997	574
Implementation Plan	Build E Installation Plan	Apr 1998	576
Implementation Plan	Build F Installation Plan	Mar 1998	579
Implementation Plan	Build F Installation Plan (CWV Draft 3, as Built)	Jun 2000	580
Implementation Plan	Early Build C Installation Plan	May 1997	583
Training Plan	ITN Training Plan	Jul 1999	587
Training Plan	Training Plan, AFIS	Nov 1998	595
Test Report	Build C Test Report, Volume 1	Aug 1997	573
Test Report	Build D Test Report, Volume 1	Dec 1997	575
Test Report	Build E Test Report, Volume 2	May 1998	578
Test Report	Build F1 Test Report, Volume 1	May 1999	581
Test Report	IAFIS System Acceptance Test Report	Aug 1999	585

The IAFIS was deployed in July 1999 based on 12-year old technology. The IAFIS is operating satisfactorily at this time; however, due to increased demand for new and existing services continual upgrades are necessary. Workload projections for FY 2008 are expected to exceed 168,000 fingerprint submissions per day. The current IAFIS design capacity is 170,000 per day. The following IAFIS enhancements are planned for FY 2008: (1) additional system capacity due to increased fingerprint submissions; (2) additional system capacity related to processing of flat fingerprint submissions in support of the Department of Homeland Security' need to expedite fingerprint processing at Ports of Entry; and (3) the automation manual processes related to update of criminal history records to streamline and improve existing services and offer new services. Additionally, four regularly scheduled IAFIS Builds occur each year for defect correction and system enhancements. Requests for change to the IAFIS baseline may be initiated internally or externally at the request of contributing agencies.

Congressional mandates, such as, the USA PATRIOT Act of 2001, the Enhanced Border Security and Visa Entry Reform Act of 2001, the DOJ Entry/Exit Border Security Proposal, propose new applications for the fingerprint-based identification services provided by the FBI's IAFIS. To achieve the goals outlined in these Acts and Proposals, enhancements to existing IAFIS functions and the development of new IAFIS related capabilities are required.

Information Assurance Technology Infusion
Federal Bureau of Investigation

IATI Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	Feasibility Study, IATI Program, CARA, Version 1.0	Mar 2005	605
Business Case Study	OMB Exhibit 300 for FY 2008	Mar 2006	612
Privacy Impact Assessment	Privacy Impact Assessment, CARA	Apr 2006	613
Risk Management Plan	Risk Management Plan (RMP), Technology Infusion Program, Version .8	Nov 2003	616
Project Plan	Program Management Plan, Technology Infusion Program, Volume I, Version .19	Nov 2003	614
Security Plan	Security Attachment to the FBI System Security Plan (SSP), IATI Program, IODM, Version 2.0	May 2006	619
Security Plan	System Security Plan (SSP), IATI Program, CARA, Version 6.0	May 2006	623
Security Plan	System Security Plan (SSP), IATI, SSIAC, SAE, Version 7.0	Mar 2006	624
Systems Engineering Management Plan	System Engineering Master Plan, IATI Program, Version 1.0	May 2004	621
Configuration Management Plan	Configuration Management Plan (CMP), Technology Infusion Program (TI), Volume 1, Version 0.5	Nov 2003	602
Quality Assurance Plan	Quality Assurance Plan (QAP), IATI, Volume 1, Version .9	Nov 2003	615
Test Plan	System Test Plan, IATI Program, CARA, Version 3.0	Jan 2006	625
Test Plan	Test and Evaluation Master Plan (TEMP), IATI, Draft	Apr 2004	626
Test Plan	Test Plan, IATI Program, IODM, Version 3.0	May 2006	627
Conversion Plan	Transition Plan, IATI Program, CARA, Version 1.0	May 2006	629
Implementation Plan	Installation Plan, IATI Program, IODM, Version 2.0	May 2006	608
Implementation Plan	System Installation Plan, IATI Program, CARA, Version 3.0	May 2006	622
Training Plan	Training Plan, IATI Program, CARA, Version 2.0	Apr 2006	628

The Information Assurance Technology Infusion (IATI) Program was initiated and began spending funds in FY 2005; the system implementation was completed in FY 2006. IATI is a Security Division initiative to design, develop, assess, and implement security technology

safeguards in the FBI's IT enterprise to mitigate risks to and reduce vulnerabilities of the Bureau's most critical information assets. IATI provides resources for research, evaluation, design, development, implementation, and operations and maintenance of IT security solutions that enhance the security for the Federal Bureau of Investigation's 340 plus information systems. Many of these systems directly enable the information sharing requirements for Intelligence, Counterterrorism, and operational missions.

Investigative Data Warehouse
Federal Bureau of Investigation

The FBI's Investigative Data Warehouse (IDW) began spending funds in FY 2002, and system implementation was completed in FY 2005. The IDW system provides data storage, database management, search, information presentation, and security services allowing FBI investigative and analytical personnel to access aggregated data previously only available through individual applications. The IDW system is the successor to the Secure Collaboration Operational Prototype Environment (SCOPE), which originally was named the Secure Counter-terrorism Operational Prototype Environment.

The IDW receives, stores, processes data in a heterogeneous computing environment of UNIX and Windows Servers. Data processing is conducted by a combination of Commercial-Off-the-Shelf (COTS) applications, interpreted scripts, and open-source software applications. Data storage is provided by several Oracle Relational Database Management Systems (DBMS) and in proprietary data formats. Physical storage is contained in Network Attached Storage (NAS) devices and component hard disks. Ethernet switches provide connectivity between components and to FBI LAN/WAN. An integrated firewall appliance in the switch provides network filtering.

Users of the system are FBI investigative, analytical, and intelligence personnel. These personnel are both FBI employees and contractors. Administrators of the system are FBI IDW program contractors. Users are permitted to access the system from FBI accredited facilities in the United States of America. IDW is not available to FBI Legal Attaché offices.

IDW Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Risk Management Plan	Risk Management Plan, IDW, Version 1.0	Feb 2005	631
Security Plan	System Security Plan, IDW, Version 2.0	May 2006	633
Conversion Plan	Transition and Deployment Plan, IDW	Jun 2004	636
Training Plan	Training Management Plan, IDW	Jun 2004	635
Test Report	Test & Evaluation Test Analysis Report (TETAR) for IDW, Version 1.1	Jul 2004	634

Law Enforcement Online
Federal Bureau of Investigation

LEO is a 24-hours-a-day, 7-days-a-week, on-line, controlled-access communications and information-sharing data repository. It provides an Internet-accessible focal point for electronic Sensitive But Unclassified (SBU) communications and information sharing for the federal, state, local and tribal law enforcement agencies. LEO also supports anti-terrorism, intelligence, law enforcement, criminal justice, and public safety communities nationwide. User anywhere in the world can communicate securely using LEO. LEO is accessed by vetted and authorized entities using industry-standard personal computers equipped with any standard Internet browser software. LEO currently supports a user base of over 40,000 individuals, who access LEO either via the Internet, dialup, or other dedicated connections. In addition to the current LEO user base, there are 17,000 potential Regional Information Sharing Systems (RISS) users who may have the ability to access LEO. LEO operates as SBU network under the Computer Security and Privacy Acts. In summary, LEO provides a mechanism for law enforcement entities to share data internally and externally.

LEO Studies, Plans, and Evaluations

Document Type	***Title***	***Date***	***Item #***
Business Case Study	OMB Exhibit 300 for BY 2008, CEI		1017
Project Plan	Implementation Plan for the LEO System Relocation of Primary Operations to the CJIS Division	May 2006	643
Project Plan	Project Management Plan, LEO, Relocation and Reengineering Project	Jun 2006	653
Security Plan	FBI LEO System Security Plan, dated 9 June 2006	Jun 2006	642
Configuration Management Plan	LEO Configuration Management (CM) Processes, dated 21 June 2004	Jun 2004	647
Test Plan	System Test Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Jun 2006	657
Conversion Plan	Transition Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Jun 2006	659
Implementation Plan	Installation Plan, LEO System Relocation of Primary Operations to the CJIS Division (Final Draft)	Dec 2005	644
Contingency/Continuity Plan	IT Contingency Plan, LEO, Version 1.0 (Draft)	May 2006	645

National Crime Information Center
Federal Bureau of Investigation

The National Crime Information Center (NCIC) is a computerized criminal justice information system available 24 hours a day, 365 days a year. NCIC is accessed by over 6 million Federal, State, and Tribal entities, including the Department of Homeland Security and the Department of Defense. The NCIC database consists of 18 files, including seven property files and eleven person files.

NCIC Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1028
Risk Management Plan	Risk Management Plan for NCIC 2000, \Revision 2	Feb 1996	684
Project Plan	Plan for Early Delivery of the FMS Subsystem, NCIC 2000 Program	Apr 1997	682
Security Plan	System Security Plan (SSP), NCIC	Jul 2006	688
Systems Engineering Management Plan	System Engineering Management Plan for NCIC 2000	May 1996	687
Configuration Management Plan	Configuration and Data Management Plan for NCIC 2000	Feb 1998	669
Test Plan	Maintainability Test Plan and Procedure for NCIC 2000	May 1999	675
Test Plan	Maintainability Test Plan for NCIC 2000	Feb 1994	676
Test Plan	Successive Level Integration Test Plan for NCIC 2000	Jul 1996	686
Test Plan	Test and Evaluation Master Plan for NCIC 2000	Mar 1996	690
Conversion Plan	Preliminary Transition Plan for NCIC,Volume I of VII, Transition Overview	Apr 1997	693
Conversion Plan	Transition Plan for NCIC 2000	Aug 1998	691
Implementation Plan	Facility Requirements and Installation Plan for NCIC 2000	Jul 1998	670
Training Plan	Personnel Requirements and Training Plan for NCIC	Nov 1998	681
Test Report	External Interface Checkout Test Report for NCIC 2000	May 1999	665
Test Report	Fingerprint Matching Subsystem Beta Test Report, NCIC 2000	May 1999	672
Test Report	FMS Reintegration Test Report for NCIC 2000	Mar 1999	673
Test Report	Maintainability Test Report for NCIC 2000	Jun 1999	677
Test Report	NCIC 2000 Security Certification and Testing Analysis	Jul 1999	678

NCIC also contains the Originating Agency Identifier (ORI) file. The NCIC ORI File contains contact information, such as the agency's address and telephone number, for agencies that have an ORI. The NCIC may also be used to search and retrieve the criminal history records of 50 subjects.

The NCIC is considered a Sensitive But Unclassified system and is subject to all DOJ and FBI policy, standards and practices governing the collection and dissemination of SBU data. Access to the NCIC system is controlled at the agency level by ORI. Authorized users are authenticated by user ID and password. Users are also required to be trained and tested on NCIC policy and practices.

The NCIC is an invaluable tool that aids law enforcement and criminal justice agency officials in the successful completion of their day-to-day operations and protect the United States from terrorist attack. The Terrorist Screening Center enters terrorist information in the Violent Gang and Terrorist Organization File (VGTOF) and maintains the documentation to support the terrorist watch-list. Additionally, the National Counterterrorism Center, the Joint Terrorism Task Forces, and the Field Intelligence Groups have electronic access to NCIC through their respective CJIS System Agency. Federal, State, local and tribal entities may search and retrieve VGTOF, and other person records, electronically by name, and a unique numeric identifier such as date of birth. Records may also be obtained as a result of a query of the Wanted Person File and Stolen Vehicle File. Finally, NCIC will send a notification to the Terrorist Screening Center whenever a fingerprint search results in a hit on a VGTOF record.

NCIC is in the operations and maintenance phase of the Life Cycle Management Directive. In FY 2008, the FBI CJIS Division will continue to upgrade hardware that has reached the end of its life-cycle and add new services such as an enhanced ad hoc search capability.

Law Enforcement National Data Exchange
Federal Bureau of Investigation

Information sharing is mission critical to today's public safety mandate. Most law enforcement agencies (LEAs) utilize some type of computerized data base to collect incident and investigative information. Moving this data across jurisdictional boundaries into the hands of those who need to know is a significant challenge. The Law Enforcement National Data Exchange (N-DEx) concept is to take the data provided by LEAs and criminal justice agencies and convert it into valuable information to fight crime and terrorism. N-DEx services extract specific information on people, places, things, the relationship between them, as well as crime characteristics such as MO's and criminal signatures.

N-DEx will: (1) share complete, accurate, timely and useful criminal justice information across jurisdictional boundaries and provide new investigative tools that enhance the United States' ability to fight crime and terrorism; (2) provide fusion centers, the National Counterterrorism Center, Field Intelligence Groups, Joint Terrorism Task Force, and other agencies with access to N-DEx capabilities and services; (3) check all new suspects entered into the system against terrorist watch lists or notify/alert users of addresses that are known to be associated with other suspected terrorists; (4) provide the capability to share sensitive investigative information while simultaneously protecting the investigative equities of proprietary information; (5) provide an electronic catalog of structured criminal justice information that provides a single point of discovery to assist in locating terrorism information and people with relevant knowledge about that information; (6) leverage its national connectivity environment to create a directory of LEAs and users to facilitate new methods of law enforcement collaboration relevant to cases, investigations, or discovered data describing terrorist activity; and (7) provide advance search capabilities to discover information when there is a lack of key information for conducting a typical query search. N-DEx will provide insights into previously unknown terrorist activity through automated discovery of patterns and linkages to detect and deter crime and terrorism.

N-DEx Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1029
Privacy Impact Assessment	Privacy Impact Assessment, N-Dex	Mar 2006	1386
Risk Management Plan	Risk Management Plan, Law Enforcement N-DEx, Version 1.4	Aug 2006	700
Project Plan	Program Plan, Law Enforcement N-Dex	Jul 2006	699
Security Plan	System Security Plan Attachment H - Risk Assessment, N-Dex Prototype, Version 1.1	Jun 2004	702
Test Plan	Certification Test Plan, N-DEx	Oct 2004	694

Next Generation Identification
Federal Bureau of Investigation

The Next Generation Identification (NGI) project began spending funds in FY 2005. The project will be a major upgrade to the current Integrated Automated Fingerprint Identification System (IAFIS) that will provide new functionality, as well as improve upon current functionality. The NGI was included in a previous IAFIS OMB 300 submission because it is a major upgrade to the existing IAFIS. In 2005, the NGI was separated from the IAFIS exhibit 300 for management control purposes based on guidance from the FBI's Office of the Chief Information Officer.

NGI Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1030
Privacy Impact Assessment	PIA, Advanced Fingerprint Identification Technology (AFIT)		719
Privacy Impact Assessment	PIA, Enhanced IAFIS Repository		720
Privacy Impact Assessment	PIA, Interstate Photo System (IPS)		721
Privacy Impact Assessment	PIA, National Palm Print System (NPPS)		722
Risk Management Plan	Risk Management Plan, NGI	Nov 2005	729
Project Plan	Project Management Plan, NGI, Version 1.0	Jan 2006	726
Configuration Management Plan	Configuration Management Plan, NGI	Apr 2006	709
Quality Assurance Plan	Quality Assurance Plan, NGI	May 2006	727
Performance Evaluation	Investment Management/Project Review Board	Feb 2006	713
Performance Evaluation	Program Management Review	May 2006	725

The NGI Program is a compilation of initiatives that will either improve or expand existing biometric identification services. The NGI Program will accommodate increased information processing and sharing demands in support of anti-terrorism. As a result of the NGI initiatives, the FBI will be able to provide services to enhance interoperability between stakeholders at all levels of government, including local, state, federal, and international partners. This will accommodate the increasing need for pre-employment background checks, licenses, and will support the increase in border patrol and entry/exit checks. The NGI will allow the FBI to: establish a terrorist fingerprint identification system that is compatible with other systems; increase the accessibility and number of the IAFIS terrorist fingerprint records; and provide latent palm print search capabilities.

The NGI Study Contract was awarded to Intellidyne, L.L.C. on July 1, 2005. Intellidyne, L.L.C. and CJIS NGI representatives jointly participated in User Requirements Canvasses which

included onsite interviews, telephonic interviews and written surveys resulting in the identification of over 1,000 new requirements, including high-priority, specialized requirements in the Latent Services, Facial Recognition, and Multi-modal Biometrics areas.

National Instant Criminal Background Check System
Federal Bureau of Investigation

The National Instant Criminal Background Check System (NICS) prevents the transfer of a firearm to persons who are prohibited from possessing or receiving a firearm while allowing the timely transfer to those individuals that are not prohibited. Title 18, Section 922 of the United States Code defines who is prohibited from shipping, transporting, possessing, or receiving any firearm or ammunition in or affecting commerce. The NICS was created through the collaborative efforts of the FBI; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Justice; local, state, and other federal law enforcement agencies; and private contractor support.

NICS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1031
Security Plan	System Security Plan, NICS/ FBI	May 1998	746
Configuration Management Plan	Configuration Management Plan, CJIS Division, Revision 1.2	Aug 2002	732
Quality Assurance Plan	Quality Assurance Plan, CJIS Division	Mar 2005	743
Test Plan	Certification Test Plan, NICS/E-Checks/NICS Call Center	Sep 2005	730
Test Plan	Formal Qualification Test Plan, NICS	Jul 1998	737
Test Plan	System Test Plan, NICS Efficiency Upgrade Project, Draft	Jun 2003	747
Conversion Plan	NICS Rehost Transition Plan	May 2004	742
Conversion Plan	Transition Plan NICS Efficiency Upgrade Project	Oct 2003	749
Implementation Plan	Installation Plan, NICS	Jun 1998	740
Implementation Plan	NICS Efficiency Upgrade Installation Plan, Draft	Sep 2003	741
Implementation Plan	Superdome System Administration and Installation Cookbook, NICS [Rehost]	Jul 2005	745
Implementation Plan	Windows 2003 Server Installation Cookbook, NICS, Revision 3.0 [Efficiency Upgrade]	Mar 2006	750
Contingency/Continuity Plan	Contingency Plan, NICS	Dec 2001	733
Contingency/Continuity Plan	Contingency Plan, NICS and E-Check	Sep 2005	735
Test Report	Formal Qualification Test Report, NICS	Oct 1998	739

The NICS Regulation, Title 28, Code of Federal Regulations, Part 25, Subpart A requires the NICS to provide Federal Firearms Licensees (FFL) with an immediate response regarding the person for whom the receipt of a firearm would violate the Code. Additionally, if the initial response is a "delay," the NICS is required to provide the FFLs with a "proceed" or "deny" response within three business days. The NICS Regulation provides the states with the option to act as a point of contact (POC) for NICS transactions and allows the FBI to serve as the POC in

those states that have chosen not to perform the checks. There are currently 13 full POC states/territories, eight partial POC state/territories, and 35 non-POC state/territories.

The NICS Regulation required development of other electronic means of contact as an alternative to the telephone. Therefore, the NICS E-Check was developed. This function enables the FFLs to initiate an unassisted NICS background check for firearm transfers via the Internet. When the FFLs conduct a NICS check, a name search is conducted for matching records in the following three databases: (1) the National Crime Information Center, which contains information on wanted persons; (2) the Interstate Identification Index, which contains criminal history records; and (3) the NICS Index, which contains the names of prohibited persons as outlined in the Brady Act.

During FYs 2006 and 2007, the NICS will undergo an extensive Business Process Re-design study to seek opportunities to improve the NICS services. FY 2008 funding will be used to finalize the results of the study, provide project management and business case support and conduct requirements development efforts.

Multi-Agency Information Sharing Initiative Regional Data Exchange
Federal Bureau of Investigation

The Multi-Agency Information Sharing Initiative (MISI) Regional Data Exchange (R-DEx) project began spending funds in FY 2005. The R-DEx is designed to provide the capability to share full text investigative information from federal, state, and local investigative agencies. R-DEx will provide searching, link analysis, and geo-spatial capabilities to aid investigators, analysts, and managers in analyzing criminal activity. It will facilitate the elimination of suspects, setting leads, and establishing linkages in cases that wouldn't otherwise occur. R-DEx is being developed in four phases. Phase I was the development of the concept of Operations, System Requirements Document, and Tool Suite that meets those requirements. Phase II was the implementation of the system as an operational prototype in St. Louis, San Diego, and Seattle. Phase III was the implementation of up to ten additional sites.

The DOJ Law Enforcement Information Sharing Program (LEISP) strategy facilities improved capabilities for law enforcement agencies to collaborate across agency, jurisdictional and geographic boundaries making that information available for use by all law enforcement agents. R-DEX fits into the LEISP data fusion category by co-mingling data on a regional level. R-DEX will provide for the collections and sharing of regional data between federal, state, local and tribal law enforcement agencies, regional FBI sites, and other federal law enforcement agencies. R-DEX development and deployment for Phase III will be coordinated with the DOJ/OCIO to ensure that development as a part of the FBI Information Sharing Initiative, designed to facilitate the sharing of information at the federal, state, and local levels, which provides an integrated approach to the development or upgrade of systems designed to share investigative information by providing powerful analytical tools for analyzing integrated datasets and making the information available to users at all levels of government. LEISP will: leverage existing system capabilities, architectural components, and business services where plausible; redirect the management and execution of projects where performance failures or weaknesses have been identified; and result in the development of a single enterprise wide information sharing architecture for the Department. LEISP is the critical DOJ-wide initiative to facilitate the sharing of what law enforcement knows about terrorism, criminal activity and threats to public safety.

R-DEx Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1032
Risk Management Plan	Risk Assessment and Risk Management Matrix (RMM), RDEX, Version 1.0	Jul 2005	662
Security Plan	System Security Plan, FBI Regional Data Exchange (R-DEx), Version 4.2	May 2006	664
Test Plan	Certification Test Plan, R-DEx, Version 1.6	Feb 2005	660
Test Report	Certification Test Report, R-DEx, Version 1.6	Feb 2005	661

Sensitive Compartment Information Operational Network
Federal Bureau of Investigation

The Sensitive Compartment Information Operational Network (SCION) began spending funds in FY 2003. The FBI is working to strengthen its capabilities to detect, analyze, understand, expose, pre-empt, interdict, terminate, and prosecute terrorist activities before they can reach the stage of causing harm to the United States. SCION will enhance these capabilities by providing agents, counter-terrorism intelligence analysis, and their staffs with modern information processing/extraction tools and unified access to relevant and appropriate data sources at the TS/SCI level.

SCION is a common TS/SCI network providing FBI users with standard applications, data sharing, and through Joint Worldwide Intelligence Communication System (JWICS), access to other intelligence community information systems. SCION primarily supports the FBI Counter Intelligence (CI) and Counter-Terrorism (CT) divisions. SCION provides the means for the divisions to access raw intelligence and intelligence products, perform analysis, and to distribute intelligence product.

SCION Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Privacy Impact Assessment	Full Privacy Impact Assessment, TS/SCI LAN	Dec 2002	751
Security Plan	System Security Plan, SCION	Aug 2004	753
Configuration Management Plan	Configuration Management Plan, SCION	Dec 2003	752
Test Report	Certification Test Results, TS/SCI LAN	May 2003	754

Sentinel
Federal Bureau of Investigation

The Sentinel project began spending funds in FY 2005 with implementation projected for FY 2010 The FBI is implementing Sentinel to replace legacy systems and to provide improvements identified in the wake of the Oklahoma Bombing Case, the terrorist attacks of September 11, and the Hanssen Espionage Case.

The FBI's investigative case management systems maintain more than 300,000 open and closed cases per year, which together contain more than 100 million text documents. However, only a subset of the information currently collected by the Bureau is being entered into the Automated Case Support (ACS) for FBI-wide access. ACS data entry processes are manually intensive, and a significant backlog for entering data into ACS exists in some locations. ACS has extremely limited capabilities for structuring the information collected by the FBI. Agents and analysts throughout the Bureau maintain case data and significant intelligence information off-line in their own internally developed or commercial-off-the shelf (COTS) applications that run on stand-alone desktops. The information residing in these systems is available only to those users that have direct system access.

SENTINEL Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Aug 2006	1033
Privacy Impact Assessment	Sentinel Phase 1 Privacy Impact Assessment	Feb 2006	1434
Risk Management Plan	Risk Management Plan, SENTINEL, Version 1.2	Jul 2005	772
Acquisition Plan	Acquisition Plan (FD-911), SENTINEL, Version 2.0	Aug 2005	755
Acquisition Plan	Source Selection Plan, FBI Sentinel Program, Version 2.95	Aug 2005	1037
Project Plan	Program Management Plan, SENTINEL, Version 1.2	Aug 2005	770
Systems Engineering Management Plan	Systems Engineering Management Plan (SEMP), SENTINEL	Jun 2005	776
Configuration Management Plan	Configuration Management Plan, SENTINEL PMO, Version 1.1	Jul 2005	758
Quality Assurance Plan	Quality Management Plan, SENTINEL, Version 1.0	Jul 2005	771
Test Plan	Test and Evaluation Master Plan (TEMP), SENTINEL	Jul 2005	777
Performance Evaluation	Lessons Learned, Sentinel, Version 1.0	Jul 2005	1039

Sentinel will put critical information in the hands of agents and analysts in the field. With few exceptions, Sentinel will provide its users with instantaneous access to all information entered into a case file. It will improve the collection and availability of information by allowing

users to create electronic documents using web-based forms. Sentinel will include a multimedia capability that will rectify a longstanding information-sharing limitation with the FBI. Agents will be able to scan documents, photographs, and other electronic media into the case file, allowing evidence and other case-related information to be shared among agents working on a case without the need to exchange physical copies of the information

Security Management Information System
Federal Bureau of Investigation

The Security Management Information System (SMIS) project began spending funds in FY 2004. SMIS is a multi-year technology initiative employing knowledge management concepts hosted on an Enterprise Service Bus compliant with the FBI's Service Oriented Enterprise Architecture to increase the ability of the FBI to develop, analyze, share, manage and store security related data in order to reduce risk to people, facilities, operations and information.

SMIS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007	Jan 2006	797
Privacy Impact Assessment	Initial Privacy Impact Assessment, Polygraph Workflow Management Application	Aug 2005	791
Privacy Impact Assessment	Initial Privacy Impact Assessment, SMIS	Aug 2005	792
Privacy Impact Assessment	Privacy Impact Assessment, Security Division Implementation the Financial Disclosure Forms Analyzer	Feb 2006	798
Risk Management Plan	Risk Management Plan, SMIS, Final 1.1	Dec 2005	817
Project Plan	Project Plan, SMIS Facilities Certification and Accreditation Component, Draft	Mar 2006	812
Project Plan	Project Plan, SMIS Financial Disclosure Forms Analyzer Component, Draft	Feb 2006	813
Project Plan	Project Plan, SMIS, Version 0.7, Draft	Jul 2005	814
Security Plan	System Security Plan, Financial Disclosure Forms Analyzer (FDF-A), Version 1.2	Jan 2006	826
Security Plan	System Security Plan, Polygraph Workflow Management System	Apr 2006	827
Configuration Management Plan	Configuration Management Plan, SMIS, PMO, Version 1.0	Jul 2005	785
Quality Assurance Plan	Quality Management Plan, SMIS, Version 1.0	Jul 2005	815
Test Plan	Certification Test Plan, FDF-A	Jan 2006	782
Test Plan	Test and Evaluation Master Plan for the Polygraph Workflow Management Application	Aug 2005	829
Test Plan	Testing and Evaluation Master Plan Unit Testing and Traceability Matrix, SMIS FCA Application	Mar 2006	831
Training Plan	Training Plan for the Polygraph Workflow Management Application	Sep 2005	833
Test Report	Certification Test Report, FDF-A	Feb 2006	783
Test Report	Test Analysis Report for the Polygraph Workflow Management Application	Nov 2005	828
Performance Evaluation	Control Gate Review Exit Report, SMIS, FDF-A, Gate 6 - OAR	Mar 2006	786

Document Type	*Title*	*Date*	*Item #*
Performance Evaluation	Investment Management/ Project Review Board (IMPRB), Summary Notes	Jan 2005	794
Performance Evaluation	Investment Management/ Project Review Board (IMPRB), Summary Notes	Aug 2005	793

The SMIS project will replace out-dated manual work processes and proliferating, stand-alone spreadsheets and databases with an efficient, cohesive, highly automated capability enabling authorized users to effectively and efficiently mine multiple security related applications, databases, and other electronically assimilated sources of relevant data to provide the Bureau with timely, actionable intelligence and security support information. Upon completion, SMIS will contain all security-related information for the entire professional life cycle of a person, facility or system. The enhanced capabilities will allow Security Division (SecD) to share selected information with other divisions, law enforcement entities, and the Intelligence Community (IC) in the most efficient manner.

Technical Refreshment Program
Federal Bureau of Investigation

The Technical Refreshment Program (TRP) project began spending funds in FY 2007. The program is an orderly and planned replacement of the FBI's technical assets associated with the FBI's FBINET and UNet enclaves, which are the primary backbones of the FBI's communications and operations. The TRP will follow the FBI's enterprise architecture technical reference model to support the technical framework. The standards, specifications, and technologies that support the delivery of service components and capabilities will be accomplished by replacing IT equipment at 20 percent per year.

The FBI has experienced information technology growth because of the new tasks forces, new data sharing initiatives, and new classified programs. The FBI currently has over 60,000 desktops, 27,000 laptops, 21,000 printers, and over 2,600 servers. The FBI requires funds to refresh and upgrade network components, enhance network functions, incorporate new network management software, and provide new features for monitoring and control. As mandated by OMB, the FBI will plan to upgrade all components to implement the FBI to IPv6 for network communications. Control and software tools will be constantly enhanced and integrated, and improve the ability of EOC personnel to manage the FBI's IT infrastructure. The improvements will enable the FBI to continue to improve the productivity and efficiency of the FBI's IT infrastructure. The program is chartered to replace aging and out of date IT Hardware to minimize obsolescence, in advance of loss of service or hardware failure. The impact, if not funded, will put the FBI at risk. This is due to the fact that the hardware cannot be serviced, as the IT industry will not support IT hardware beyond its 5th year of service.

TRP Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1034
Performance Evaluation	Project Summary Report, TRP		836

Terrorist Screening Center
Federal Bureau of Investigation

The Terrorist Screening Center (TSC) project began spending funds in FY 2004. The project was formed by the Department of Justice in response to Homeland Security Presidential Directive-6 (HSPD-6), dated 16 September 2003. The TSC originates and maintains the United States' only consolidated terrorist identities database, participates in and explores ways to improve information sharing with all defense, national security, intelligence and law enforcement partners, as well as select foreign partners, and initiates and leads the Federal Search Working Group.

The TSC supports national security by providing information on both international and domestic terrorist identities on demand for agencies and/or Departments, including the Department of State, the Department of Homeland Security's Customs and Border Protection and Transportation Security Administration, granting access on the basis of need-to-know to the limit prescribed by the originating agency of record. The TSC's links with many communities, including law enforcement at the state, local, tribal and territorial levels, are maintained around the clock.

TSC Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2008	Dec 2006	1035
Risk Management Plan	Risk Management Plan, Terrorist Screening Center (TSC), Version 1.7 (Draft)	Apr 2006	845
Project Plan	TSDB Automated Ingest Project Plan	Apr 2006	849
Security Plan	System Security Plan, TSDB Phase 1B, Version 1.2		846
Verification/Validation Plan	Independent Verification and Validation (IV &V) Plan, TSC		848
Test Plan	Independent Verification and Validation (IV &V) Plan, TSC		848
Test Plan	Test Management Plan, TSDB 1.7.1	Mar 2006	847
Test Report	IV & V Test Report, TSDB 1.8.0.2, TSC	May 2006	843

The TSC's basic philosophy is of information sharing with all partner agencies, and participation in monthly information sharing sessions with partner agencies and foreign government representatives. The TSC hosts regular training for all employees, to include sensitive but unclassified classifications and privacy issues. Despite budget constraints, improvements in efficiency and functionality are ongoing and necessary to obtain the full scope of HSPD-6 and meet the mandate of the President's Management Agenda. The TSC uses the very latest search and retrieval technologies to meet these requirements, and is pioneering search technology in several areas, most notably search standards through development of a control database, search "cocktails" by the use of a combination of multiple search engines, and the federation of searches to search several databases at one time.

In budget year 2008, the TSC plans to develop an ability for external users to query the Terrorist Screening Database (TSDB), as well as a portal for external users to better reach and share and exchange information with the TSC call center, intelligence and nominations personnel. The query capability will be in production by early FY 2008, with the portal to follow. Future efforts will include improved data consumption of NCTC into the TSDB, deployment of biometric capability, planned hardware and software interface with DHS, Voiceprint and DNA data, and improved privacy and security features within EMA supporting TSDB.

Classified Information Technology Program
Justice Management Division

Components Involved: All components except FBI

CITP Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Enterprise Proof-of-Concept Functional Requirements, JSIT, Version 1.1	Dec 2003	154
Business Case Study	Fiscal Year 2005 Information Technology Concept Paper		158
Business Case Study	OMB Exhibit 300 for BY 2006		173
Privacy Impact Assessment	Initial Privacy Impact Assessment, JCON-S		161
Privacy Impact Assessment	Initial Privacy Impact Assessment, JCON-TS		162
Privacy Impact Assessment	Privacy Threshold Analysis, JCON-S		175
Privacy Impact Assessment	Privacy Threshold Analysis, JCON-TS		176
Risk Management Plan	Risk Assessment/Risk Matrix, JWICS	Dec 2003	180
Risk Management Plan	Risk Management Plan, Enterprise SIPRNET, Draft	Mar 2003	181
Risk Management Plan	Risk Management Plan, JIST, Version 1.0, Draft	Jul 2006	182
Acquisition Plan	Acquisition Plan, CITP, Version 1.0	Jan 2006	142
Project Plan	MOA between JCON and DTO Regarding Operation and Support of the JCON Classified Infrastructure, Version 0.2, Draft	Dec 2003	171
Project Plan	Program Guide, JCON-S, Version 2.1	May 2005	177
Security Plan	System Security Authorization Agreement (SSAA), JCON-S	Feb 2004	188
Security Plan	System Security Plan, JWICS Network, JCON-TS	Dec 2003	189
Configuration Management Plan	Configuration Management Process, JCON-S, Appendix V, Version 1.1	Dec 2003	147
Configuration Management Plan	Published Documents, Configuration Management Plan, JCON-S, Version 1.0	May 2004	146
Verification/Validation Plan	Engagement Security Approach, JCON-S		153
Test Plan	Acceptance Test Plan and Report	Dec 2003	168
Test Plan	Security Test and Evaluation Plan, JCON-S, Appendix E	Feb 2004	186
Conversion Plan	Data Migration, ADNET to JCON-S		150
Implementation Plan	Sample JSIT Deployment Plan		151

Document Type	*Title*	*Date*	*Item #*
Training Plan	Computer Security Awareness and Training (C/SAT) Plan, JCON-S Enterprise System, Version 2.1	Dec 2003	145
Contingency/Continuity Plan	Contingency Plan, JCON-S, Appendix L	Feb 2004	149
Contingency/Continuity Plan	Contingency Plan, JWICS Network, Appendix M		148
Test Report	Acceptance Test Plan and Report	Dec 2003	168
Test Report	Security Test and Evaluation Plan, JCON-S, Appendix E	Feb 2004	186

The Classified Information Technology Program (CITP) project began spending funds in FY 2003. The mission is to develop a Department of Justice Classified Enterprise Architecture, an initial operational infrastructure, and an Operations and Maintenance Model for processing classified information. The scope of the project includes classified information technology for all Department of Justice components except the Federal Bureau of Investigation. The project's objectives are to: (1) define requirements to support implementation of a Department Sensitive Compartmented Information and Collateral Classified Information Processing Capability; (2) implement initial capabilities for Top Secret/Sensitive Compartmented Information and Collateral Classified Information Processing Capability; and (3) define an ongoing program for Department of Justice Classified Information Technology.

Integrated Wireless Network
Justice Management Division

Components Involved: All Components

The Integrated Wireless Network (IWN) project began spending funds in FY 2001. The project is a collaborative effort by the Departments of Justice, Homeland Security, and the Treasury to provide a consolidated, nationwide federal wireless communications service that replaces stovepipe stand alone component systems, and supports law enforcement, first responder, and homeland security requirements with integrated communications services in a wireless environment.

IWN Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Market Research Summary	Apr 2004	1388
Business Case Study	High Level Design Report		198
Business Case Study	OMB Exhibit 300 for BY 2007	Jan 2006	206
Risk Management Plan	Risk Management Plan, DOJ Wireless Management Office, Justice Wireless Network	Jun 2006	211
Acquisition Plan	Acquisition Plan, IWN JPO	Aug 2004	195
Project Plan	Program Plan FY 2006, Joint Program Office, Draft	Jun 2005	209
Project Plan	Strategic Plan 2005-2010, Integrated Wireless Network (IWN), (Draft)	Jun 2006	1004
Security Plan	System Security Plan, Beta Test System	Nov 2004	214
Configuration Management Plan	Configuration Management Plan, JPO IWN	Jun 2004	196
Quality Assurance Plan	Quality Assurance Plan, DOJ Wireless Network		210
Verification/Validation Plan	Data System Functional Tests, JPO-Pilot System	Oct 2004	192
Verification/Validation Plan	Network Management	Oct 2004	193
Verification/Validation Plan	Report Generation Tests	Oct 2004	194
Test Plan	Data System Functional Tests, JPO-IWN Pilot System	Oct 2004	192
Test Plan	Network Management	Oct 2004	193
Test Plan	Report Generation Tests	Oct 2004	194
Test Plan	Security Test and Evaluation Report: Beta Test System	Nov 2004	213
Implementation Plan	Organizational Readiness Transition Activities, IWN Seattle-Blaine Service Area	Sep 2004	203
Implementation Plan	Transition Plan	Oct 2004	215

Document Type	*Title*	*Date*	*Item #*
Training Plan	Personnel Training for the Integrated Wireless Network	Nov 2004	208
Contingency/Continuity Plan	Contingency Plan, JPO IWN Northwest Zone	Jun 2005	197
Performance Evaluation	Beta Benchmark Assessment, IWN Seattle/Blaine		202
Post-Implementation Evaluation	Beta Benchmark Assessment, IWN Seattle/Blaine		202

The IWN will implement solutions to provide federal agency interoperability with appropriate links to state, local, and tribal public safety, and homeland security entities. Justice, Treasury and DHS personnel represent the majority of law enforcement personnel within the Federal Government and are responsible for fulfilling numerous duties related to national law enforcement, protective missions, and homeland security missions. These operations are made more effective, efficient, and safe through the use of tactical communications. Unfortunately, current legacy wideband networks do not have sufficient communications capabilities to support the successful accomplishment of core activities. Many of the existing systems are 15 years old or older and are increasingly unreliable and expensive to maintain. Furthermore, varying tactical communications systems exist between field offices and organizations, preventing basic interoperability and presenting logistical issues during the course of routine enforcement activities. This incompatibility of systems makes communications interoperability difficult to achieve.

To meet these challenges, the IWN design is based on a very high frequency, Project 25 trunked system utilizing a packet switched Internet Protocol backbone. Additionally, the system design provides for encrypted communications. The network is presently based on land mobile radio services, and may be complemented by commercial wireless service solutions. The IWN will also be designed to facilitate interoperability with other federal, state and local public safety partners.

Justice Consolidated Office Network
Justice Management Division

Components Involved: Antitrust Division, Civil Division, Civil Rights Division, Community Relations Service, Criminal Division, Environment and Natural Resources Division, Executive Office for Immigration Review, Executive Office for United States Attorneys, Federal Bureau of Prisons, Justice Management Division, Office of Justice Programs, Tax Division, U. S. Marshals Service, U. S. Trustee Program, U. S. National Central Bureau of INTERPROL, U. S. Parole Commission

The JCON program began in FY 1996. The program provides a standard, consolidated DOJ Enterprise Office Solution, in partnership with DOJ components and the Office of Chief Information Officer's staff, through the delivery of standing technology products and services. JCON is the critical infrastructure that provides a reliable and robust common office automation platform upon which 16 of the Department's litigating, management, and law enforcement components operate their mission-critical applications. The cornerstone of the JCON is the JCON Standard Architecture, which defines the basic information technology computing framework, including networked workstations, servers, printers, a common set of core applications, such as email and word processing, and a basic set of system administration tools. JCON also provide the infrastructure for components to access case management and other mission-related databases, e-Gov applications, and the Department's law enforcement, litigation, and administration systems. JCON provides the fundamental IT tools and services required by Department employees and contractors to perform their daily work functions.

JCON Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	JCON Architecture Study, Final Report	Jan 1998	227
Market/Other Research	Request for Information (RFI), JCON PMO, Version 1.0	Apr 2006	1012
Business Case Study	OMB Exhibit 300 for BY 2007	Dec 2005	387
Privacy Impact Assessment	Initial Privacy Impact Assessment		380
Privacy Impact Assessment	Privacy Threshold Analysis		390
Risk Management Plan	Risk Management Plan, JCON PMO, Version 2	Jul 2003	400
Acquisition Plan	Contract Administration, JCON		374
Project Plan	Project Management Plan Template, JCON PMO SDLC, Version 2.0	May 2005	391
Project Plan	Project Management Plan, Civil Rights Division, JCON Implementation	Dec 2005	392
Project Plan	Project Management Plan, EOUSA JCON IIA Deployment	May 2005	393
Project Plan	Project Management Plan, JCON Modernization	Jun 2005	394
Project Plan	Strategic and Tactical Plan, JCON	Apr 2005	1005

Document Type	*Title*	*Date*	*Item #*
Security Plan	System Security Plan, JCON-COAR	May 2006	404
Systems Engineering Management Plan	Systems Engineering Process, JCON PMO, Version 1.0	Jun 2006	407
Configuration Management Plan	Configuration Management Plan, JCON PMO, Version 1.2	Mar 2006	372
Test Plan	System Test Plan for DOJ EOIR, Version 1.0, Draft	Aug 2005	405
Test Plan	System Test Plan Template, JCON PMO SDLC, Version 1.0	Mar 2005	406
Implementation Plan	Implementation Plan, EOIR, Final Version 2.7	May 2006	379
Implementation Plan	JCON Implementation Plan Template and Guidance, JCON PMO SDLC, Version 2.0	Mar 2005	382
Contingency/Continuity Plan	Contingency Plan, JCON COAR, Version 1.8	Mar 2006	373
Test Report	Security Test and Evaluation, JCON COAR	May 2006	401
Test Report	System Analysis Report JCON Civil Rights Division Design, Version 1 - Final	Apr 2006	403
Performance Evaluation	Department Executive Review Board Presentation	Feb 2005	375
Post-Implementation Evaluation	Civil Rights Division Lessons Learned Report, JCON IIA Implementation Phase	May 2006	371
Post-Implementation Evaluation	Lessons Learned Report for the JCON Civil Deployment Implementation Phase	May 2006	385
Post-Implementation Evaluation	Lessons Learned Report Template and Guidance, JCON PMP SDLC, Version 1.0	Jan 2005	386
Post-Implementation Evaluation	Summary of Findings, Email Users Survey	Dec 2005	402

Litigation Case Management System
Justice Management Division

Components Involved: Executive Office for United States Attorneys
Antitrust Division
Civil Division
Civil Rights Division
Criminal Division
Environment and Natural Resources Division
Tax Division

The Department's major litigating components are highly decentralized, with information stored in numerous disconnected systems. The Litigation Case Management System (LCMS) initiative will develop and implement a common case management solution for the litigating components that will support efficient, automated information sharing and streamlined reporting capabilities. The project is part of the Department's Case Management Common Solutions and OMB's Lines of Business Programs to develop business-driven, common solutions across agencies. The LCMS will consist of a suite of solutions built on a common foundation, creating a case management architectural blueprint, data standards, and other products that should be reusable by other agencies. (The OMB-300 for budget year 2007 indicates that several components were in various stages of pursing their own solutions, and are now participating in the LCMS program.)

The LCMS project began spending funds in FY 2003 and is planned to be phased in incrementally, beginning with Phase 1 in FY 2007 in U.S. Attorney's Offices. Phase 1 is intended to incorporate case information management and reporting, workload management, and time reporting. Litigation support tools that can be used by attorneys to organize and manage individual cases are not part of Phase 1.

LCMS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Final Market Research Report, LCMS	Jun 2005	250
Business Case Study	OMB Exhibit 300 for BY 2007	Dec 2005	252
Business Case Study	Technical Evaluation Report, LCMS Phase 1, Version 0.9, Final	Apr 2006	256
Privacy Impact Assessment	Privacy Impact Assessment (Draft)	May 2005	1383
Project Plan	Project Management Plan, Version 1.2	Aug 2005	254
Configuration Management Plan	Project Configuration Management Plan, Version 1.1	Apr 2005	253

Public Key Infrastructure
Justice Management Division

Components Involved: All Components

The Department of Justice has established a Public Key Infrastructure Program (PKI) to provide infrastructure-level trust services to enhance existing and planned business processes, applications, and services. The PKI will enhance security in order to foster communication between Department personnel across Components, other Federal, State, and Local Government agencies, commercial business partners, and transactions involving private citizens. The PKI is not in itself a security service, but instead is an underlying infrastructure-level service that enhances the offerings of existing security services within the DOJ enterprise. To augment these security services, the PKI Program will seek to establish an enterprise-wide public key capability and look to enable key business processes to leverage the services provided by the DOJ PKI.

PKI Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Planning and Design Support, DOJ PKI	Oct 2002	232
Business Case Study	Business Case, DOJ Enterprise PKI, Version 1.0	Jul 2004	216
Business Case Study	OMB Exhibit 300 for BY 2008, CEI		1017
Privacy Impact Assessment	Privacy Threshold Analysis (questionnaire)		235
Project Plan	Project Management Plan, DOJ PKI	Aug 2004	236
Security Plan	System Security Plan, DOJ PKI, Revision 2	Mar 2006	244
Configuration Management Plan	Configuration Management Plan, DOJ PKI Program and Technical Support, Version 1.1, Draft	Mar 2005	220
Test Plan	Test and Evaluation Master Plan, DOJ PKI, Revision 1	Apr 2005	245
Implementation Plan	Deployment Implementation Plan, DOJ PKI, Final	Jun 2005	222
Training Plan	Training Plan, DOJ PKI, Final	Apr 2005	247
Disposition Plan	Chain of Custody Processes, DOJ PKI, Version 1.01	Jun 2005	218
Contingency/Continuity Plan	IT Contingency Plan, DOJ PKI, Appendix L, Revision 3	Mar 2006	226
Test Report	Security Test and Evaluation Plan (Final), DOJ PKI	May 2005	242
Test Report	Test Report, DOJ PKI, Draft	Jun 2005	246
Performance Evaluation	Earned Value Management, DOJ Enterprise PKI Infrastructure Service Office		223

Unified Financial Management System
Justice Management Division

Components Involved: All components

The Department of Justice has initiated an effort to implement a unified system that will improve the existing and future financial management and procurement operations across DOJ. The Department will address these needs via the implementation of the Unified Financial Management System (UFMS), which is planned to replace six core financial management systems and multiple procurement systems currently operating across DOJ with an integrated commercial off the shelf solution.

UFMS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Market/Other Research	Financial Vendor Response Summary Draft		1418
Business Case Study	OMB Exhibit 300 for BY 2007	Dec 2005	99
Privacy Impact Assessment	Privacy Impact Assessment, UFMS, Working Draft	Dec 2006	1399
Risk Management Plan	Risk and Issue Management Plan, Version 2.0	Sep 2004	101
Acquisition Plan	Acquisition Plan UFMS Integration and Implementation Services	Jun 2005	86
Acquisition Plan	Acquisition Strategy Paper, DOJ UFMS	Jun 2002	87
Project Plan	DOJ Program Office Charter and Program Management Plan, Version 2.0	Sep 2004	93
Project Plan	Implementation and Integration - Project Management Plan, Version 1.0	Jun 2006	94
Security Plan	Security Management Plan (UFMS), Version 2.0	Jan 2006	103
Security Plan	System Security Plan (SSP) for DOJ UFMS	Dec 2005	105
Systems Engineering Management Plan	Integration and Implementation - Systems Engineering Plan	Jul 2006	96
Configuration Management Plan	Configuration Management Plan, Version 1.0	Aug 2005	88
Configuration Management Plan	Configuration Management Plan, Version 2.0	Jun 2006	89
Quality Assurance Plan	Integration and Implementation - Quality Control Plan, Version 1.0	Jul 2006	95
Test Plan	Integration and Implementation Test and Evaluation Master Plan	Jul 2006	97
Conversion Plan	Data Conversion Strategy, Version 1.0	Jul 2006	92
Implementation Plan	System Implementation Plan, Version 1.0	Jul 2006	106
Training Plan	Training Strategy, Version 1.0	Jul 2006	109

The UFMS will allow the DOJ to streamline and standardize business processes and procedures across all components, providing accurate, timely, and useful financial data to

financial and Program managers across the Department, and produce component- and Department-level financial statements. In addition, the system will assist the DOJ by improving financial management performance and aid Department components in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security identified by the OIG. Finally, the system will provide procurement functionality, consolidated management information, and the capability to meet all mandatory requirements of the Federal Acquisition Regulation and the Justice Acquisition Regulations.

Justice Grants Management System
Office of Justice Programs

Components Involved: Office of Justice Programs
Office of Community Oriented Policing Services

The Justice Grants Management System (JGMS) is a web based, data driven application that provides end-to-end support for the application, approval, and management of grants for the proposed Justice Grants Management Consortium. JGMS is adaptable to accommodate the varying grants processes and grants types of its multiple users. JGMS supports the core missions and grants processes of DOJ's Office of Justice Programs and Office on Violence Against Women, and is targeted to incorporate the Community Oriented Policing Services (COPS) program. The Office of Grants and Training, Department of Homeland Security is also an established JGMS user and will continue to be supported by JGMS.

JGMS Studies, Plans, and Evaluations

Document Type	*Title*	*Date*	*Item #*
Business Case Study	OMB Exhibit 300 for BY 2007		364
Project Plan	Grant Adjustment Notice (GAN) Module Project Management Plan, Draft	Sep 2005	360
Security Plan	System Security Plan for Grants Management System	Feb 2006	340
Configuration Management Plan	Configuration Management Plan, OJP	Nov 2004	341
Test Plan	GAN Module Test Plan, OJP		347
Test Plan	GMS Grant Adjustment Notice Module Test Cases	Oct 2005	346
Test Plan	Grant Adjustment Notice Module Test Plan, Phase 2		348
Training Plan	GMS GAN Training Plan, (Draft)	May 2005	359
Contingency/Continuity Plan	Continuity of Operations Plan, OJP	Jul 2005	342
Test Report	Functional Requirements Document, Grant Adjustments, OJP, Version 1.1	Nov 2005	345
Test Report	GAN Test Problem Report (Spreadsheet)		357
Test Report	Validation Test Script Forms, GMS	Feb 2006	1390

The Justice Grants Management Consortium formalizes the existing alliance of JGMS users, with the addition of new users with like interests such as COPS. JGMS has the capability to accommodate additional prospective agencies whose missions support first responder and disaster grants programs, should they elect to join the Consortium as members. JGMS provides an interface with the Grants.gov portal to allow potential applicants to conduct searches and apply for DOJ and Department of Homeland Security grant opportunities using the Grants.gov Find and Apply capabilities. JGMS will also build upon its interface with the financial

management system which accounts for its DOJ users' grant funds and disburses funds to grantees, and its capability to export financial-related grants transaction data to external financial systems.

APPENDIX VII

PRIOR OIG REPORTS

Performance Audits and Inspection Reports

Report Number	Report Title
04-36	The Drug Enforcement Administration's Management of Enterprise Architecture and Information Technology Investments
05-01	The Bureau of Alcohol, Tobacco, Firearms and Explosives and Federal Bureau of Investigation's Arson and Explosives Intelligence Databases
05-07	Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project
05-22	The Joint Automated Booking System
05-27	Review of the Terrorist Screening Center
05-30	Bureau of Alcohol, Tobacco, Firearms, and Explosives National Integrated Ballistic Information Network Program
05-32	Processing Classified Information on Portable Computers in the Department of Justice
05-34	Review of the Terrorist Screening Center's Efforts To Support the Secure Flight Program – Limited Official Use
06-02	The Status of Enterprise Architecture and Information Technology Investment Management in the Department in the Department of Justice
06-14	The Federal Bureau of Investigation's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System
06-25	Inventory of Major Department of Justice Information System Investments as of FY 2006
06-33	The Federal Bureau of Investigation's Implementation of the Laboratory Information Management System
07-03	Sentinel Audit II: Status of the Federal Bureau of Investigation's Case Management System Redacted
07-25	Progress Report on Development of the Integrated Wireless Network in the Department of Justice
I-2005-001*	Follow-up Review of the Status of the IDENT/IAFIS Integration
I-2006-007*	Follow-up Review of the FBI's Progress Toward Biometric Interoperability Between IAFIS and IDENT

* Denotes an inspection report prepared by the OIG Inspections Division.

Federal Information Security Related Audits

Report Number	Report Title
05-16	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - United States Marshals Service's Automated Prisoner Scheduling System
05-21	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - Drug Enforcement Administration's Investigative Management Program and Case Tracking System (IMPACT)
05-23	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - United States Marshals Service's Information Security Program
05-26	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - Federal Bureau of Investigation's Tactical Operations Unit Network (TOUNET) – Secret
05-29	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - Drug Enforcement Administration's Information Security Program – Limited Official Use
05-31	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2004 - Federal Bureau of Investigation's Information Security Program – Limited Official Use
06-01	Independent Evaluation Pursuant to the Federal Information Security Management Act – Fiscal Year 2004- Department's Information Technology Security and Oversight Program – Limited Official Use
06-20	Independent Evaluation Pursuant to the Federal Information Security Management Act - FY 2005 - Department of Justice's Justice Management Division Information Security Program and Oversight – Limited Official Use
06-22	Independent Evaluation Pursuant to the Federal Information Security Management Act – Fiscal Year 2005 - Federal Bureau of Investigation's Automated Case Support Application - Secret
06-23	Independent Evaluation Pursuant to the Federal Information Security Management Act - FY 2005 - Federal Bureau of Investigation's Information Security Program – Secret
06-27	Independent Evaluation Pursuant to the Federal Information Security Management Act - Fiscal Year 2005 - The Department of Justice's Drug Enforcement Administration Information Security Program - Limited Official Use
06-28	Independent Evaluation Pursuant to the Federal Information Security Management Act – Fiscal Year 2005 - The Department of Justice's Federal Bureau of Prisons' Inmate Telephone System II
06-29	Independent Evaluation Pursuant to the Federal Information Security Management Act – Fiscal Year 2005 - The Department of Justice's Federal Bureau of Prisons' Information Security Program

Report Number	Report Title
06-31	Independent Evaluation Pursuant to the Federal Information Security Management Act – Fiscal Year 2005 - The Drug Enforcement Administration's El Paso Intelligence Center Seizure System

Financial Statement Related Audits

Report Number	Report Title
05-03	Department of Justice Annual Financial Statement Fiscal Year 2004
05-05	Working Capital Fund Annual Financial Statement Fiscal Year 2004
05-06	Offices, Boards and Divisions Annual Financial Statement Fiscal Year 2004
05-08	Federal Bureau of Investigation Annual Financial Statement Fiscal Year 2004
05-09	Federal Prison Industries, Inc., Annual Financial Statement Fiscal Year 2004
05-11	Bureau of Prisons Annual Financial Statement Fiscal Year 2004
05-12	Assets Forfeiture Fund and Seized Asset Deposit Fund Annual Financial Statement Fiscal Year 2004
05-13	United States Marshals Service Annual Financial Statement Fiscal Year 2004
05-14	Drug Enforcement Administration Annual Financial Statement Fiscal Year 2004
05-15	Bureau of Alcohol, Tobacco, Firearms and Explosives Annual Financial Statement, Fiscal Year 2004
05-17	Office of Justice Programs Financial Statement Fiscal Year 2004
05-35	Review of the Federal Bureau of Investigation Headquarters' Information Systems Control Environment Fiscal Year 2004 – Secret
05-36	Office of Justice Programs Annual Financial Statement Fiscal Year 2003 As Restated
05-38	Office of Justice Programs Annual Financial Statement Fiscal Year 2004 As Restated
06-04	The Department of Justice Annual Financial Statement Fiscal Year 2005
06-05	Offices, Boards and Divisions Annual Financial Statement Fiscal Year 2005
06-06	Federal Bureau of Investigation Annual Financial Statement Fiscal Year 2005
06-07	Asset Forfeiture Fund and Seized Asset Deposit Fund Annual Financial Statement Fiscal Year 2005
06-09	United States Marshals Service Annual Financial Statement Fiscal Year 2005
06-10	Drug Enforcement Administration's Annual Financial Statement Fiscal Year 2005
06-12	Working Capital Fund Annual Financial Statement Fiscal Year 2005

Report Number	Report Title
06-17	Office of Justice Programs Annual Financial Statement Fiscal Year 2005
06-18	Federal Prison Industries, Inc., Annual Financial Statement Fiscal Year 2005
06-19	Federal Bureau of Prisons Annual Financial Statement Fiscal Year 2005
06-21	Bureau of Alcohol, Tobacco, Firearms and Explosives Annual Financial Statement Fiscal Year 2005
06-24	Department of Justice Review of the Consolidated Information System General Controls Environment - Fiscal Year 2005 - Limited Official Use
07-08	Office, Boards and Divisions Annual Financial Statement Fiscal Year 2006
07-09	Federal Bureau of Investigation Annual Financial Statement Fiscal Year 2006
07-11	Drug Enforcement Administration Annual Financial Statement Fiscal Year 2006
07-21	Office of Justice Programs Annual Financial Statement Fiscal Year 2006

DEPARTMENT'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Washington, D.C. 20530

JUL 24 2007

MEMORANDUM FOR FERRIS B. POLK
REGIONAL AUDIT MANAGER
ATLANTA REGIONAL AUDIT OFFICE

FROM: Vance E. Hitch
Chief Information Officer

SUBJECT: Response to Draft Audit Report of the Department of Justice Information Technology Studies, Plans and Evaluations

We have received and reviewed your Draft Audit Report - Department of Justice Information Technology (IT) Studies, Plans and Evaluations, dated July 3, 2007.

Each of the report's recommendations is addressed below:

Recommendation 1 - Evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing IT studies, plans, and evaluations for individual IT projects.

OCIO Response - We concur. The Department of Justice (DOJ) Office of the Chief Information Officer (OCIO) will review selected projects in Appendix VI, System Summaries, in the subject audit report. The purpose of this review will be to ascertain the rationales used by the DOJ component IT project managers for preparing certain studies, plans, and evaluations. Based on this review, the Department will consider revising the current guidelines for preparing studies, plans, and evaluations.

Recommendation 2 - Consider revising the guidelines for tailoring the work pattern for specific types of projects.

OCIO Response - We concur. The DOJ OCIO will conduct an evaluation of the various IT project types that currently exist at the Department using a variety of criteria as input to the evaluation (e.g., cost, risk etc.) and will develop standard work patterns and deviations/waivers for each project type.

Recommendation 3 - Ensure that post-implementation and post-termination evaluations are conducted that focus on lessons learned for project planning and management.

OCIO Response - We concur. As part of the Evaluate Phase in the Capital Planning and Investment Control (CPIC) process, the Department plans to implement a Post Implementation Review (PIR) process. The PIR process will follow guidance provided by OMB in the Capital Programming Guide. The PIR will most likely occur six months after a system has been in operation or immediately following system termination. The review will provide a baseline as to whether to continue the system without adjustment; to modify the system to improve performance; or if necessary, to consider alternatives to the implemented system. Some common elements that will be reviewed during the PIR include:

a. Mission alignment
b. IT architecture including security and internal controls
c. Performance measures
d. Project management
e. Customer acceptance
f. Business process support
g. Financial performance
h. Return on investment
i. Risk management
j. Select and control phase performance ensuring initiative success
k. Gaps or deficiencies in the process used to develop and implement the initiative
l. Best practices that can be applied to other IT initiatives or the CPIC process

The Department Investment Review Board (DIRB) will select the IT projects that will require a PIR review.

Recommendation 4 - Ensure that staff receive training to obtain skills needed to adequately direct and oversee contractor efforts.

OCIO Response - We concur. In Fiscal Year 2004, the Department and its components validated the qualifications of the IT project managers for the major DOJ IT projects using the OMB Federal IT Project Manager Guidance matrix. The matrix was used to determine whether each project manager for a major IT project possessed the necessary competencies and suggested work experience to manage the major IT project assigned to them. The

Department reviews the qualifications of the IT project managers for the major DOJ IT projects during the Exhibit 300 review process each year. In addition, all IT project managers are required to be certified as Contracting Officers' Technical Representatives (COTRs). IT project managers are required to be re-certified as COTRs every five years.

Recommendation 5 - Implement targeted reviews to improve the use of business process re-engineering and requirements analysis early in concept development.

OCIO Response - We concur. The Department will implement review criteria to ensure that business process re-engineering and requirements analysis are effectively incorporated early into the concept development phase of project planning. Targeted reviews will be conducted at the discretion of the DIRB.

If you have any questions, please contact John Murray on (202) 305-9635.

APPENDIX IX

INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

The OIG provided a draft of this audit report to the Department for review and comment. The Department's response of July 24, 2007, included in this report as Appendix VIII, concurs with the five recommendations and proposes corrective action sufficient to resolve all the recommendations. Our analysis of the response to the recommendations is provided below.

1. **Resolved**. We recommended that the Department's CIO evaluate why project teams do not prepare certain plans and evaluations, reassess the utility of those documents, and consider revising the standards for producing studies, plans, and evaluations for individual IT projects. The Department's response indicates the OCIO will review selected projects to determine the rationales for preparing certain studies, plans, and evaluations, and consider revising the current guidelines. This recommendation is resolved based on the planned action, but the Department did not provide a specific timeframe for the process to be completed. The Department should provide a specific timeframe for this process to be completed, and the recommendation can be closed when we receive documentation of the results of this review.

2. **Resolved.** We recommended that the CIO consider revising the guidelines for tailoring the work pattern for specific types of projects. The Department's response indicated the OCIO will conduct an evaluation of the various IT project types and will develop standard work patterns and deviations or waivers for each project type. This recommendation is resolved based on the planned actions, but the Department did not provide a timeframe for the process to be completed. The OCIO should provide a specific timeframe for the process to be completed, and the recommendation can be closed when we receive documentation of the results of this effort.

3. **Resolved.** We recommended that the CIO ensure that post-implementation and post-termination reviews are conducted that focus on lessons learned for project planning and management. This recommendation is resolved based on the CIO's plans to implement a post implementation review process that will follow guidance in the Office of Management and Budget's *Capital Programming Guide*. The Department did not provide a specific timeframe for the process to be implemented. The Department should provide a specific timeframe for

this process to be implemented, and the recommendation can be closed when we receive documentation demonstrating that this process has been implemented.

4. **Resolved.** We recommended that the CIO ensure that staff receive training needed to direct and oversee contractor efforts adequately. This recommendation is resolved based on the CIO's response that the qualifications of the IT project managers for major IT projects are now reviewed each year during the exhibit 300 review, and that all IT project managers are now required to be re-certified as contracting officers' technical representatives every 5 years. The recommendation can be closed when we receive documentation of: (1) the FY 2004 validation of project manager qualifications, (2) the procedures used for review of project manager qualifications, and (3) the requirement that project managers be certified and re-certified as contracting officers' technical representatives.

5. **Resolved.** We recommended that the CIO implement targeted reviews to improve the use of business process re-engineering and requirements analysis early in concept development. This recommendation is resolved based on the Department's plan to implement review criteria to ensure that business process re-engineering and requirements analysis are effectively incorporated early into the concept development phase of project planning, and that targeted reviews will be conducted at the discretion of the Department Investment Review Board. The Department did not provide a specific timeframe for these actions to be implemented. The Department should provide a specific timeframe for these actions to be implemented, and the recommendation can be closed when we receive documentation that the actions have been implemented.