

U.S. Department of Justice

**FY 2012 Performance Budget
Congressional Justification**

Justice Information Sharing Technology

Table of Contents

	Page No.
I. Overview.....	3
II. Summary of Program Changes.....	4
III. Appropriations Language and Analysis of Appropriations Language.....	5
IV. Decision Unit Justification	
A. Justice Information Sharing Technology.....	6
1. Program Description.....	6
2. Performance Tables.....	15
3. Performance, Resources, and Strategies.....	17
a. Performance Plan and Report for Outcomes.....	17
b. Strategies to Accomplish Outcomes.....	18
c. Results of Program Assessment.....	18
V. Program Offsets.....	19
VI. Exhibit	
A. Organizational Chart	
B. Summary of Requirements	
C. Program Increases/Offsets by Decision Unit	
D. Resources by DOJ Strategic Goal/Objective	
E. Justification for Base Adjustments	
F. Crosswalk of 2010 Availability	
G. Crosswalk of 2011 Availability	
H. Summary of Reimbursable Resources	
I. Detail of Permanent Positions by Category	
J. Financial Analysis of Program Changes	
K. Summary of Requirements by Grade	
L. Summary of Requirements by Object Class	

I. Overview for Justice Information Sharing Technology (JIST)

The FY 2012 JIST request includes \$54,307,000 and a total of 72 positions. JIST funds the Department of Justice (DOJ) enterprise investments in Information Technology (IT). As a centralized fund under the control of the DOJ Chief Information Officer (CIO), it ensures that investments in IT systems, information sharing technology, enabling IT infrastructure enhancements, and cyber security are well planned and aligned with the Department's overall IT strategy and enterprise architecture. Given the level of staff dependence on the Department's IT environment (systems, networks, and data archives), CIO oversight is critical to the Department's legal, investigative, and administrative functions and to the maintenance and improvement of DOJ staff productivity and effectiveness. Electronic copies of the Department of Justice's Congressional Budget Justification and Capital Asset Plan and Case exhibits can be viewed or downloaded from the Internet using the Internet address:
<http://www.justice.gov/02organizations/bpp.htm>.

In FY 2012, the JIST appropriation will fund the Office of the CIO's performance of responsibilities under the Clinger-Cohen Act of 1996, the Department's response to OMB mandates, and nine programs that support the overall mission of the Department and contribute to the achievement of DOJ strategic goals. The nine JIST funded programs are:

- Investigation, law enforcement, litigation and intelligence
 - Joint Automated Booking System (JABS)
 - Law Enforcement Information Sharing Program (LEISP)
 - Chief Technical Officer – Technology Innovations (CTO)
- Security and Secure Communications
 - Cyber Security Program (CSP)
 - Secret / Top Secret Communications (JCON S/TS)
 - Public Key Infrastructure/HSPD-12 (PKI)
- Critical Enabling IT Infrastructure
 - Justice Consolidated Office Network (JCON)
- Financial Management
 - Unified Financial Management Systems (UFMS)
- DOJ IT Management and Innovation
 - Policy & Planning Staff (PPS)

Linkage to Strategic Goals

JIST programs directly support the three Strategic Goals that are included in the Department's FY 2007-2012 Strategic Plan. These are:

- Strategic Goal 1: Prevent terrorism and promote the nation's security.
- Strategic Goal 2: Prevent crime, enforce federal laws, and represent the rights and interests of the American People.
- Strategic Goal 3: Ensure the fair and efficient administration of justice.

In addition to the above three Strategic Goals, DOJ recognizes "Strategic Goal 4: Enabling administration" as a fourth Strategic Goal. It allows and enables staff and other programs to pursue the other Strategic Goals in an effective and efficient manner.

II. Summary of Program Changes

Item Name	Description			Page
	Pos.	FTE	Dollars (\$000)	
Operations	0	0	(\$11,500)	19
Realign and Consolidate PMOs	0	0	(\$ 5,000)	21
Extend Tech Refresh	0	0	(\$ 443)	23
Administrative Efficiencies	0	0	(\$ 13)	24

III. Appropriation Language and Analysis of Appropriation Language

A. Appropriation Language

For necessary expenses for information sharing technology, including planning, development, deployment, and departmental direction, \$54,307,000 to remain available until expended.

Note. – A full-year 2011 appropriation for this account was not enacted at the time the budget was prepared; therefore, this account is operating under a continuing resolution (P.L. 111-242, as amended). The amounts included for 2011 reflect the annualized level provided by the continuing resolution.

B. Analysis of Appropriation Language

“No substantive changes proposed.”

Note: The FY 2012 President’s Budget uses the FY 2011 President’s Budget language as a base so all language is presented as new.

IV. Decision Unit Justification

A. Justice Information Sharing Technology – (JIST)

JIST - TOTAL	Permanent Positions	FTE	Amount
2010 Enacted	72	72	88,285,000
2011 CR	72	72	88,285,000
Adjustments to Base and Technical Adjustments	0	0	(17,022,000)
2012 Current Services	72	72	71,263,000
2012 Program Offsets	0	0	(16,956,000)
2012 Request	72	72	54,307,000
Total Change 2011-2012	0	0	(33,978,000)

JIST-Information Technology Breakout	Permanent Positions	FTE	Amount
2010 Enacted	72	72	88,285,000
2011 CR	72	72	88,285,000
Adjustments to Base and Technical Adjustments	0	0	(17,022,000)
2012 Current Services	72	72	71,263,000
2012 Program Offsets	0	0	(16,956,000)
2012 Request	72	72	54,307,000
Total Change 2011-2012	0	0	(33,978,000)

1. Program Description

The JIST appropriation funds enterprise IT investments and supports programs in the following areas:

- Investigation, Law Enforcement, Litigation, and Intelligence
- IT Security and Secure Communications
- Critical Enabling IT Infrastructure
- Financial Management
- DOJ IT Management and Innovations

These Programs provide enterprise-wide security infrastructure and cyber security monitoring, secure communications, and IT applications to provide modern and secure IT environments to support the daily activities of the Department's agents, attorneys, analysts, and administrative staff. In addition, JIST funds the performance of Departmental responsibilities assigned to the CIO by the Clinger-Cohen Act of 1996, including the implementation of a capital planning and investment control process, the development and maintenance of an information technology architecture, the establishment of IT performance measures and IT security programs, and the development of strategies for improving information resources management.

a. Investigation, Law Enforcement, Litigation and Intelligence

Joint Automated Booking System (JABS)

The JABS Program is a field-proven, mission critical law enforcement system responsible for capturing, processing, managing, and sharing prisoner and detainee booking and tracking information. It is charged with providing information interchange services that eliminates the need to perform redundant bookings when prisoners are moved within DOJ.

The Program provides the provisioning and operational maintenance for 1,100 Automated Booking Stations (ABS) within the DOJ and manages the electronic data interfaces with the FBI's Integrated Automated Fingerprint Identification System (IAFIS). Including booking stations maintained by DHS and the USMS's Inter-Agency booking functionality, JABS services approximately 2,500 Federal law enforcement sites. JABS, which operates 24/7, has an estimated 64,000 registered users who submit over 2 million transactions per year to IAFIS. The JABS program currently accounts for 87% of the Federal electronic booking transactions submitted to IAFIS. These booking submissions provide a "real-time" update to the FBI's fingerprint and criminal history databases.

The JABS has a significant role in counterterrorism and law enforcement since it provides booking information, including applicable scars, marks, and tattoo data, to counterterrorism and law enforcement fusion centers through OneDOJ. The JABS data repository currently consists of more than 3 million booking records, which is cited by the law enforcement community as being extremely effective in assisting them to accomplish their mission. Additionally, JABS provides data extracts to the Organized Crime Drug Enforcement Task Force (OCDETF) fusion center, DEA-Pinellas County, FL. Sheriff's Office facial recognition pilot fusion center, and the Arizona Counter Terrorism Information Center (ACTIC).

Law Enforcement Sharing Program (LEISP)

LEISP represents a strategic approach to sharing data with other DOJ components, other federal agencies, and partners at the state, local, and tribal levels. The program aims to reduce crime and to prevent terrorism by providing an overall framework and the technological means for law enforcement entities to share information quickly and effectively. It promotes the continued development and implementation of information sharing systems that enable state, local, and Federal law enforcement agencies nationwide to collect, share, and analyze law enforcement information on criminal activities and separately, in a more tightly controlled environment, to share and analyze sensitive intelligence data.

LEISP is an executive oversight program that provides the lynchpin for connecting several ongoing projects within key DOJ components, under a common set of goals and objectives, and to ensure compliance with applicable DOJ policies and memoranda that include but is not limited to data sharing, privacy, and technologies. JIST supports the development and implementation of LEISP-related database application systems that enable state, local, and Federal law enforcement agencies nationwide to collect, share, and analyze law enforcement information on criminal activities and separately, in a more tightly controlled environment, to share and analyze sensitive intelligence data.

Chief Information Officer – Technology Innovations

The CTO identifies and pilots innovative new technologies that can result in more cost-effective IT solutions for the Department, with the goal of proving their value propositions and finding Department entities to commit to adoption. Currently, the CTO is working on solutions in the following areas:

- **Data Standards:** Developing and implementing standard information structures and exchange standards that enable information exchange between federal, state, local, and tribal enforcement and intelligence organizations.
- **Identity & Access Management:** Developing a cost-effective approach for providing common, scalable, identity authentication, and access management services across the DOJ enterprise.
- **Information Sharing Infrastructure:** Developing tools and techniques that enable or facilitate information sharing with DOJ's federal, state, and local partners.
- **Information Fusion:** Collaboratively building best-of-breed prototypes for fusion capabilities such as Search and Correlation and sharing lessons learned with major DOJ programs.
- **Geospatial Information Services (GIS):** Developing enterprise GIS Infrastructure Services to greatly reduce the cost and effort to implement secure access to commercially available GIS applications and initiatives across the Department.

b. IT Security and Secure Communications

Cyber Security Program (CSP)

The Department has established two complementary programs – the Justice Security Operations Center (JSOC) and the Cyber Security Program (CSP) - to protect its IT environments (systems, networks, and sensitive data) from cyber attacks to ensure their availability for the Department's agents, attorneys, analysts, and administrative staff to continue their legal, investigative, and administrative functions. The JSOC is funded by the Department's Working Capital Fund. It proactively monitors and maintains situational awareness of the Department's networks, investigates incidents, and develops signatures to block further intrusions. The CSP JIST-funded activity is undertaking a multi-year program to implement DOJ enterprise-wide security architecture to secure networks and consolidate internet gateways.

The effectiveness of the JSOC to proactively defend against and respond to a cyber attack depends on establishing a limited number of Internet access points, the Trusted Internet Connections (TIC), having advanced monitoring capabilities and situational awareness, and an enterprise-wide security infrastructure. The CSP will establish the TIC, provide advanced situational awareness of the Department's IT environment, and secure the Department's networks by:

- Modernizing intrusion detection systems (IDS) and firewalls across DOJ, including component networks,
- Providing common mandatory server/computer settings that are managed centrally to enable more timely and coordinated responses to security threats,
- Implementing secure remote access and advanced authentication solutions that support the many needs of our agents, attorneys, and analysts,

- Implementing secure infrastructure capabilities to provide the continued processing of critical systems and networks,
- Implementing advanced malware detection capabilities to assist the JSOC in responding to the advanced persistent threat,
- Implementing a centrally-managed, departmental email system capable of hosting end-user email accounts for the greatest number of components, and
- Segmenting message traffic by type to allow JSOC to customize data monitoring and apply specific countermeasures for each traffic type.

In addition to securing the Department's networks, CSP will support the JSOC by establishing a secure communications facility to support the exchange of information with USCERT and the Intelligence Community to enhance DOJ's ability to identify and respond to incidents caused by evolving cyber threats. The secure communication facility will allow JSOC to leverage the advance collection and analysis capabilities of USCERT and the Intelligence Community, to use these capabilities to proactively secure the Department's systems and networks, and to work collaboratively on analyses and countermeasures for ongoing security incidents.

The Department's ability to achieve its strategic goals depends heavily on its ability to capture, process, manage, analyze, and share information. To meet mission investigative and information sharing requirements, DOJ's agents, attorneys, and analysts are increasingly reliant on connectivity to the Internet to enable collaboration with multiple levels of government. This connectivity level increases the exposure of DOJ systems to disruption from cyber threats and attacks. The complementary JSOC and CSP programs directly support the Department's Strategic Goals by providing DOJ with an effective security structure to counter current and emerging cyber threats and to ensure that our agents, attorneys, and analysts can continue using the Department's IT systems and networks to support their missions without significant interruption of service resulting from cyber attacks.

JCON-Secret and JCON-Top Secret (JCON-S/TS)

The Department did not have a system for secure classified intra/inter-departmental data communications at the time of the September 11, 2001 terrorist attack. In response to the significant increase in classified mission needs after the September 11, 2001 terrorist attack, the Department initiated the JCON-S/TS Program to implement a secure communications to provide seamless Information Technology (IT) infrastructure for electronically sharing, processing, and storing information classified at the Secret and Top Secret/Sensitive Compartmented Information (TS/SCI) Levels.

These classified networks are major enablers in allowing investigators, intelligence analysts, and attorneys at DOJ locations across the country and around the world to use and share classified case data. These networks use existing DOJ wide area networks, while connecting to other agencies via the worldwide backbone router networks Secret Internet Protocol Routing Network (SIPRNet) and Joint Worldwide Intelligence Communication Systems (JWICS)) operated by the Department of Defense. Currently, JCON-S/TS systems support over 3,000 DOJ component and other federal agency users at over 400 locations within the United States and associated U.S. Territories from the Virgin Islands to Guam. Since inception, the JCON-S/TS have been a critical element of the Department's Continuity of Government and Continuity of Operations plans. The increasing amount of classified investigations and litigations are causing the work stations, locations, and services to increase year over year.

JIST funds the JCON-S/TS software and hardware at user and central data center sites and the JCON-S/TS Program Management Office responsible for planning, acquiring, and implementing of this software and hardware.

Public Key Infrastructure (PKI)

The PKI program is DOJ's Identity Management Services Program which consolidates several related cyber security initiatives by developing enterprise architecture policies, plans, best practices, and standards for HSPD-12 and the Federal Identity, Credential, and Access Management (ICAM) segment architecture investments and related IT improvements across DOJ. This program provides the planning, training, operational support, and oversight of the HSPD-12 Personal Identification Verification card (PIVCard) deployment process and operates the ongoing centralized system for DOJ component employees and contractors.

The PIVCard is the centerpiece of the HSPD-12 PIVCard solution being implemented government-wide. Standards set by the National Institute of Standards and Technology (NIST) are the basis for satisfying identification and security requirements and for the use of a common PIVCard to achieve both logical and physical access to Federal-controlled facilities and information systems. The PIVCard contains logical elements including PKI certificates, digital photos, and fingerprint biometrics. The PIVCard and related processes will greatly enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

The program serves as DOJ's departmental issuer of PIVCards which is a mandatory element of the Department's compliance with government standards, and will allow cross-agency secure communications. Additionally, the program serves as the primary governing body for DOJ compliance and implementation of ICAM. This includes the development and implementation of enterprise services required to use PIVCards, and coordination and execution of agency and sub-agency ICAM implementation plans. Compliance with the Federal ICAM will ensure value is derived from the HSPD-12 PIVCard investment through increased security of agency facilities and information assets.

The key values of the overall program are the following:

- Managing DOJ-wide federal ICAM compliance, participation, and represent DOJ in government-wide security and access programs.
- Establishing a single, authoritative authentication mechanism for DOJ which will expedite (single sign-on) and expand secure access to critical information,
- Enabling identity authentication prior to accessing facilities and information systems,
- Creating related infrastructure services at DOJ to provide for digital signatures and end-to-end encryption of sensitive law enforcement and terrorist related information, and
- Supporting information access and sharing by upgrading the IT infrastructure (Enterprise Directory, enterprise messaging, stovepipe component infrastructures, and enterprise networking) to support secure communications, especially between persons from different organizations.

c. Critical Enabling IT Infrastructure

Justice Consolidated Office Network (JCON)

The JCON program provides architecture guidance and funding to build reliable, secure office automation systems and component infrastructure (desktops, laptops, servers, local area networks and data storage) upon which 16 DOJ litigation, management, and law enforcement components operate their mission-critical applications. JCON promotes interoperability and information sharing among DOJ components and their business partners, *e.g.*, courts, other components, and federal agencies, by providing for the maintenance of standard architecture and service templates, operating commonly-used office automation services, centralized acquisition management, a standardized system development and implementation methodology, configuration management, and financing for new system deployments. The key elements of the DOJ JCON strategy to maintain secure office automation systems are to:

- Establish a central, shared service offering which provides components with interoperable directory, email, collaboration, mobile computing, and desktop services,
- Promote a JCON desktop standard and associated technologies,
- Establish a predictable technology refresh cycle to ensure that all JCON components have current, secure, and compatible messaging technologies that enable collaboration within the Department, as well as with other law enforcement agencies.

Increasingly, DOJ systems and networks are required to meet stringent security and operating parameters, including additional record management requirements, encryption and data auditing, scanning requirements, new common DOJ applications, and OMB mandates. The JCON Program is critical for the Department to address and fund the requirements to support the more stringent current parameters for security and operations.

Since 2005, JCON has pursued a course to standardize requirements by developing JCONext, a suite of centralized enterprise-class systems to support multiple components with common office automation needs. This includes Enterprise Directory systems, Enterprise Email and messaging platform, Enterprise monitoring, management and help desk, Enterprise-wide desktop imaging, and others. Implementation of these centralized systems enhances the capability of the Department to develop an effective and less expensive cyber defense program, while providing a more cost effective platform for the delivery of key office automation services. The first component was migrated to JCONext in FY 2009, with JMD, USPC, CRS and SMOs following in FY 2010-2011.

d. Financial Management

Unified Financial Management System (UFMS)

The Department's Unified Financial Management System (UFMS) is one of the highest management priorities in the Department. In order to continue implementing the remaining DOJ components and to align funding for operations and maintenance, funding is being transferred to the users of UFMS on a pro rata basis. Specifically, base funding of \$17,572,000 is being transferred from the Justice Information Sharing Technology appropriation to DEA, FBI, BOP, USMS and ATF. On an annual basis, the transferred funds will be reimbursed back to the Justice Management Division's UFMS Program Management Office (PMO) to cover PMO-related

expenses in support of component implementations and for recurring operations and maintenance support.

DEA	\$3,463
FBI	9,433
BOP	697
USMS	2,806
ATF	1,173
Total (\$000)	\$17,572

Identified by the Department's Inspector General as "one of the most important challenges for the Department," the Department is implementing a Unified Financial Management System (UFMS) that will replace legacy financial systems operated by individual components. The UFMS will replace six (6) core financial management systems and multiple procurement systems currently operating across the Department with an integrated Commercial Off-The-Shelf (COTS) solution. This will allow the Department 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 Department by improving financial management performance and aid in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security identified by the Department's Inspector General. UFMS directly supports the Attorney General's top priority to "ensure the transparent, accountable, and depoliticized administration of justice." UFMS also directly supports Strategic Goal 3: Ensure the Fair and Efficient Administration of Justice included in the Department's Strategic Plan, FYs 2007 – 2012.

DOJ's objectives are to standardize core accounting processes, data, and interfaces, and to provide a centrally maintained, secure and integrated financial and acquisitions solution based on commercial software. UFMS provides the basic structure for fiscal stewardship, accountability and transparency for DOJ and component leadership, and in reporting to our external constituents. The consolidation of data reporting reduces dependence on manual processes, allows financial management personnel to spend more time analyzing financial data for decision making, and provides senior leadership with more timely management information for decision making. UFMS delivers a standard business solution consisting of 28 Department-wide business processes, 22 external interfaces, and flexible reporting based on standard data.

UFMS integrates the following core accounting functions that are configured in a standard supporting infrastructure:

- Manage General Ledger and Generate Financial Statements
- Establish Budget and Monitor Execution
- Procurement to Payment
- Reimbursable Activity/Receivable to Collection
- Manage Cash and Investments
- Performance and Cost Management
- Reporting

UFMS provides the Department and components with the ability to more accurately track finances through a Standard General Ledger (SGL); easily prepare budgets and breakdown the budget levels; reduce time between approval stages of processes, such as the procurement to payment and reimbursable activities; and accurately manage costs and investments.

The UFMS will allow the DOJ to streamline and standardize business processes and procedures across all components, providing secure, accurate, timely, and useful financial and procurement data to program managers across the Department, and produce component and Department level financial statements. In addition, the system will assist the DOJ by improving procurement and financial management performance and aid department components in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security. Finally, the system will provide fully integrated financial and procurement functionality to streamline business processes, provide consolidated management information, and the capability to meet all mandatory requirements of the Federal Acquisition Regulation and the Justice Acquisition Regulations.

UFMS is an ongoing initiative to incrementally implement core accounting. In December 2010, UFMS is in a mixed lifecycle phase including operations (over 2,500 users world-wide), and implementations that are underway. A pilot implementation completed in 2008 is still in operation for the Asset Forfeiture Program (AFP). The Drug Enforcement Administration (DEA) successfully implemented UFMS in January 2009. The Alcohol, Tobacco, Firearms, and Explosives (ATF) went live on the system, staying on schedule and on budget in October 2010. Three implementations are in process: AFP Phase 2 and U.S. Marshals Service (USMS) began their implementation activities and are targeting a Go Live date in early 2012. The Federal Bureau of Investigation's (FBI) Phase 2 has also begun implementation activities and is targeting a Go Live date in early 2013.

e. DOJ IT Management

OCIO-DOJ IT Management

JIST funds the Policy & Planning Staff (PPS) that supports CIO management in complying with the Clinger-Cohen Act and other applicable laws, rules, and regulations for federal information resource management. PPS develops, implements, and oversees an integrated approach for effectively and efficiently planning and managing DOJ's information technology resources. PPS performs these responsibilities by managing the following Department-wide processes: CIO Council, Department Investment Review Board (DIRB), IT Strategic Planning, IT Audits, Enterprise Architecture, IT Governance, IT Investment, and Paperwork Reduction Act program.

PPS includes groups responsible for IT investment management (ITIM), enterprise architecture (EA) and infrastructure architecture (IA). The ITIM planning and governance group manages the Department's IT investment and budget planning processes, develops and maintains the Department's general IT program policy and guidance documents, and coordinates the activities of the Department IT Investment Review Board and Department CIO Council for the Department CIO. Other responsibilities include managing the Department's Paperwork Reduction Act program, coordinating IT program audits, and ensuring IT program compliance with records management, accessibility, and other statutory requirements.

EA monitors and ensures compliance with OMB and GAO enterprise architecture requirements, advises the CIO on strategic priorities, and works to drive these priorities to implementation. To achieve these objectives, the chief enterprise architect undertakes/monitors IT strategic planning,

documents the Department-wide EA, performs EA governance/coordination across the department, supports investment reviews (DIRB and ITIM), and develops detailed architectures for Department-wide segments, such as information sharing, in collaboration with key stakeholders from across the Department. EA also works with various cross-government programs to represent the Department on issues which affect IT architecture, such as Green IT and information sharing.

IA is the tactical side of EA. This group is responsible for coordinating the Department's infrastructure initiatives; coordinating the Department's participation in OMB infrastructure initiatives such as data center consolidation, cloud computing, and power consumption reduction; performing assessments of enterprise infrastructure; and providing IA consultation with PMOs. To execute these responsibilities, IA conducts Department level reviews and analyses, validates technical approaches with respect to architecture, assesses development and deployment approaches, makes recommendations for improving DOJ infrastructure performance and cost efficiency, and prepares technical analyses and reports for the Department CIO and external authority.

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)											
DOJ Strategic Goal/Objective: Overall Mission Support Thru IT / Protecting America from the threat of terrorism											
WORKLOAD/ RESOURCES		Final Target		Actual		Projected		Changes		Requested (Total)	
		FY 2010		FY 2010		FY 2011 CR		Current Services Adjustments and FY 2012 Program Change		FY 2012 Request	
Workload											
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)		FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		72	88,285 [163,430]	72	88,285 [52,984]	72	88,285 [121,865]	0	-33,978 [-99,152]	72	54,307 [22,713]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2010		FY 2010		FY 2011 CR		Current Services Adjustments and FY 2012 Program Change		FY 2012 Request	
Program Activity		FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		72	88,285 [163,430]	72	88,285 [52,984]	72	88,285 [121,865]	0	-33,978 [-99,152]	72	54,307 [22,713]
Performance Measure	Percentage of offenders booked through JABS	99%		98%		98%		N/A		98%	
Performance Measure	Percentage of total JCON workstations deployed in the fiscal year (non-cumulative)	100%		36%		100%		N/A		100%	
Performance Measure	Maintain mainframe enterprise system availability for client organizations	99%		99%		99%		N/A		99%	
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations	99%		99%		99%		N/A		99%	
Performance Measure	Ensure IT systems are certified and accredited	100%		100%		100%		N/A		100%	
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms	75%		90%		75%		N/A		75%	

PERFORMANCE MEASURE TABLE

Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)

Performance Report and Performance Plan Targets		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010		FY 2011	FY 2012
		Actual	Target	Actual	Target							
Performance Measure	Percentage of offenders booked through JABS	N/A	N/A	95%	97%	99%	99%	98%	99%	98%	98%	98%
Performance Measure	Percentage of total JCON workstations deployed in the fiscal year (non-cumulative)	N/A	N/A	N/A	45%	0%	15%	100%	100%	36%	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	N/A	N/A	N/A	N/A	100%	100%	99%	99%	99%	99%	99%
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations	N/A	N/A	100%	99%	100%	100%	99%	99%	99%	99%	99%
Performance Measure	Ensure IT systems are certified and accredited	N/A	N/A	91%	22%	100%	100%	100%	100%	100%	100%	100%
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms	N/A	N/A	N/A	N/A	87%	78%	75%	75%	90%	75%	75%

N/A = Data unavailable

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

JIST provides resources so that the DOJ CIO can ensure that investments in IT systems, information sharing technology, and cyber security are well planned and aligned with the Department's overall IT strategy and enterprise architecture. It also directly finances certain enterprise investments in infrastructure improvements and cyber security.

Oversight of these resources and key programs is critical to their success and ensuring outcomes that support the Department's mission.

In FY 2006, the Department established a Department IT Investment Review Board (DIRB). Members of the DIRB are composed of the DOJ executive officers, augmented by non-voting DOJ representatives and component members. The Deputy Attorney General (DAG) chairs the board, and the DOJ CIO serves as vice chair. The DIRB is composed primarily of members with IT subject matter and financial management expertise, thereby providing complementary perspectives on the best use of resources to improve the management of IT investments of the Department.

The DIRB provides the highest level of investment oversight as part of the Department's overall IT investment management process. The Department's IT investments are vetted annually through the budget submission process, in conjunction with each component's Information Technology Investment Management (ITIM) process. Of the hundreds of projects that are funded annually across the Department, approximately a dozen are selected each year for DIRB review based on the size of their budget and/or their strategic importance to the Department's missions. The DIRB's principal functions in fulfilling its decision-making responsibilities are to:

- Ensure compliance with the Clinger-Cohen Act and all other applicable laws, rules, and regulations regarding information resources management,
- Monitor the Department's most important IT investments throughout their project lifecycle to ensure goals are met and the expected returns on investment are achieved,
- Ensure each project under review has established effective budget, schedule, operational, performance, and security metrics that support the achievement of key project milestones,
- Review the recommendations and issues raised by the components' IT investment management process,
- Review annually each component's IT investment portfolio, including business cases for new investments, to enable informed departmental IT portfolio decisions,
- Develop and implement decision-making processes that are consistent with the purposes of the DIRB, and with applicable Congressional and OMB guidelines for selecting, monitoring, and evaluating information system investments (these processes shall be designed to ensure that the DIRB's decisions are consistent, valid, and actionable, support the Department's business needs and processes, align with the Department's strategic goals and objectives, comply with enterprise architecture, and consider the delivery of a modernized IT infrastructure and efficient, effective services as a driving goal), and
- Establish a communication plan that conveys DIRB actions and progress against the Department's identified processes and goals.

In addition to the DIRB, the Department has established an IT Dashboard that allows management to review various aspects of major initiatives across the Department. The Dashboard is considered another oversight tool since all projects cannot be reviewed by the DIRB. The dashboard includes Earned Value Management System (EVMS) reporting, to ensure projects are evaluated against acceptable variances for scope, schedule, and costs. Risk analysis and project funding information are also available in this tool. This allows the Department's CIO and senior management team to have timely access to project information via the web.

b. Strategies to Accomplish Outcomes

Specific mission critical IT infrastructure investments are designed, engineered, and deployed with JIST resources.

- The complementary JSOC and CSP programs provide for the implementation and maintenance of an enterprise-wide security architecture to reduce the number of Internet access points and deploy an in-depth cyber attack defense strategy to lessen the effectiveness and impact of external cyber attacks, with the capability to conduct end-to-end monitoring of data traffic flows and to take defensive actions when and where necessary.
- LEISP creates the core law enforcement information sharing services that will allow information to be routinely exchanged between agencies and their systems. Its objectives are to:
 - Integrate several existing or newly initiated DOJ funded information sharing systems,
 - Direct the integration and support the timely completion of ongoing projects by infusing project coordination guidance, technology direction, and project oversight from the Office of the CIO,
 - Provide access to other federal, state, and local agency communications infrastructure to exchange law enforcement information. This will be achieved by connecting (or enhancing existing connections) between DOJ networks (JUTNET, CJIS, WAN, LEO) and the networks of other federal partners such as the Department of Homeland Security (DHS), as well as selected state/local networks such as the National Law Enforcement Telecommunications System (NLETS) and the Regional Information Sharing System (RISS).
- The JCON Program is a mature infrastructure program that provides a reliable and robust common office automation platform upon which 16 of the DOJ litigating, management, and law enforcement components operate their mission-critical applications. JCON centrally funds and manages the planning, acquiring, and implementing of a commercial-off-the-shelf (COTS) product-based office automation solution for participating components across the Department.
- JABS is a nationwide automated booking system for DOJ law enforcement agencies and serves as the information sharing system that eliminated redundant successive bookings, and established a federal offender tracking system by enabling agencies to share and exchange booking information. It is the Department's "front end" to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) which provides an automated process for the collection and transmission of fingerprint, photographic, and biographical data. JABS enables agencies to share and exchange booking information and maintain federal offender tracking capability.
- The PKI program was started by consolidating several security related initiatives. The program develops the enterprise architecture policies, best practices and standards for HSPD-12 investment, and IT improvements across DOJ and provides planning, training, operational support, and oversight of the Personal Identification Verification card (PIVCard) deployment process for DOJ component employees and contractors. The PIVCard contains logical elements including PKI certificates, digital photos, and fingerprint biometrics and will be used by government employees and contractors for achieving both logical and physical access to Federal controlled facilities and information systems.

c. Results of Program Assessment

JIST has not been selected for a Program Assessment Review.

V. Program Offsets by Item

1. Operations Reductions

Budget Decision Unit(s): JIST
 Strategic Goal(s) & Objective(s): Goal 1 – Prevent terrorism and promote the nation’s security
 Goal 2 – Prevent crime, enforce federal laws, and represent the rights and interest of the American people
 Goal 3 – Ensure the fair and efficient administration of justice
 Goal 4 -- Enabling administration
 Organizational Programs: CSP, LEISP, PKI, and PPS
 Programs Reduction: Positions 0 FTE 0 Dollars \$11,500,000

Description of Item

Realign the CSP, LEISP, PKI and PPS Program’s business operational and financial goals to achieve cost savings and review and evaluate operations and maintenance costs to identify change opportunities to increase operating efficiencies and reduce cost.

Summary Justification

The OCIO will review and evaluate the each Program’s (CSP, LEISP, PKI, and PPS) business operational and financial plans to identify opportunities to decrease cost while continuing support of the Department’s Strategic Goals. In addition, the OCIO will review and evaluate operating and maintenance costs within and across Programs to identify change actions to increase efficiency and save cost.

Impact on Performance

CSP, LEISP, PKI, and PPS support the Department’s four Strategic Goals: Goal 1 - Prevent terrorism and promote the nation’s security, Goal 2 - Prevent crime, enforce federal laws, and represent the rights and interests of the America People, Goal 3 - Ensure the fair and efficient administration of justice, and Goal 4 - Enabling administration. Cost reduction actions will be identified and implemented with a view to minimize the impact on system availability and security and the performance of other DOJ components, or on other agencies outside of DOJ, that depend on these Programs to execute their missions.

Funding

Base Funding

Program	FY 2010 Enacted			FY 2011 CR			FY 2012 Current Services		
	Pos	FTE	(\$000)	Pos	FTE	(\$000)	Pos	FTE	(\$000)
CSP	5	5	\$16,036	5	5	\$16,036	5	5	\$16,086
LEISP	3	3	\$ 4,300	3	3	\$ 4,300	3	3	\$ 4,331
PKI	7	7	\$ 6,000	7	7	\$ 6,000	7	7	\$ 6,059
PPS	25	25	\$ 6,930	25	25	\$ 6,930	25	25	\$ 7,171
Total	41	41	\$33,266	41	41	\$33,266	41	41	\$33,647

Personnel Reduction Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Reduced	FY 2012 Request (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Total Personnel		0	0	0	0

Non-Personnel Reduction Cost Summary

Non-Personnel Item	Unit Cost (\$000)	Quantity	FY 2012 Request (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Total Non-Personnel	(\$11,500)	N.A.	(\$11,500)	0	0

Total Request for this item

	Pos	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Current Services	58	58	\$ 6,774	\$26,873	\$33,647		
Decreases				(\$11,500)	(\$11,500)		
Grand Total	58	58	\$ 6,774	\$15,373	\$22,147		

V. Program Offsets by Item (continued)

2. Realign and Consolidate PMOs

Budget Decision Unit(s): JIST
 Strategic Goal(s) & Objective(s): Goal 1 – Prevent terrorism and promote the nation’s security
 Goal 2 – Prevent crime, enforce federal laws, and represent the rights and interest of the American people
 Goal 3 – Ensure the fair and efficient administration of justice
 Organizational Program: JABS, JCON, and JCON S/TS
 Offset Amount: Positions 0 FTE 0 Dollars \$5,000,000

Description of Item

Realign and consolidate the JABS, JCON, and JCON S/TS Programs to achieve savings through efficiency, economies of scale, common project management skills, methodology, and processes across the Programs.

Summary Justification

Each of these Programs has an assigned leader with skills and knowledge to address the uniqueness of its mission, users, software applications, and security requirements and to meet ongoing and changing mission demands and technology requirements. The three leaders report to the same Deputy-CIO responsible for oversight and coordination of the Programs. The OCIO will conduct a review and evaluation to identify cost savings through efficiency improvements and economies of scale that can be realized by sharing administrative functions, as well as advisory and other services, across the Programs.

Impact on Performance

JABS, JCON, and JCON S/TS support the Department’s three Strategic Goals: Goal 1 - Prevent terrorism and promote the nation’s security, Goal 2 - Prevent crime, enforce federal laws, and represent the rights and interests of the America People, and Goal 3 - Ensure the fair and efficient administration of justice. Cost reduction actions will be identified and implemented with a view to minimize the impact on system availability and security and the performance of other DOJ components, or on other agencies outside of DOJ, that depend on these Programs to execute their missions.

Funding

Base Funding

Program	FY 2010 Enacted			FY 2011 President’s Budget			FY 2012 Current Services		
	Pos	FTE	(\$000)	Pos	FTE	(\$000)	Pos	FTE	(\$000)
JABS	7	7	\$ 9,600	7	7	\$ 9,600	7	7	\$ 9,669
JCON	7	7	\$20,179	7	7	\$20,179	7	7	\$20,248
JCON S/TS	4	4	\$ 5,500	4	4	\$ 5,500	4	4	\$ 5,531
Total	18	18	\$35,279	18	18	\$35,279	18	18	\$35,448

Personnel Reduction Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Reduced	FY 2012 Request (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Total Personnel		0	0	0	0

Non-Personnel Reduction Cost Summary

Non-Personnel Item	Unit Cost (\$000)	Quantity	FY 2012 Request (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Total Non-Personnel	(\$5,000)	N.A.	(\$5,000)	0	0

Total Request for this Item

	Pos	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)	FY 2013 Net Annualization (change from 2012) (\$000)	FY 2014 Net Annualization (change from 2013) (\$000)
Current Services	17	17	\$ 2,704	\$32,744	\$35,448	0	0
Decreases				(\$ 5,000)	(\$ 5,000)	0	0
Grand Total	17	17	\$ 2,704	\$27,744	\$30,448	0	0

V. Program Offsets by Item (continued)

3. Extend Tech Refresh (PC workstations)

Budget Decision Unit:	JIST
Strategic Goal(s) & Objective(s):	Goal 4 – Enabling administration
Organizational Program:	All JIST Programs
Programs Reduction:	Positions <u>0</u> FTE <u>0</u> Dollars <u>\$443,000</u>

Description of Item

Extend tech refresh cycle for desktop/laptop PC workstations by one year.

Summary Justification

Since most current generation desktop and laptop PC workstations used by staff and consultants have fast processors, large RAMs, and large hard drives, they have excess capacity relative to their primary use for running basic office automatic applications (e.g., spreadsheets and word processing). Therefore, extending the refresh cycle by one year will have minimal impact, if any, on the users executing their normal work program, as desktops and laptops PC workstations are used primarily for basic office automation.

In FY 2012, the Department will implement the extension of refresh cycle for all desktops and laptop PC workstations. The allocated JIST share of the cost savings (offset) is (\$443,000).

Impact on Performance

As desktops and laptops PC workstations are used primarily for basic office automation applications (e.g., spreadsheets and word processing), extending the refresh cycle by one year will have minimal impact on the Department's performance.

V. Program Offsets by Item (continued)

4. Administrative efficiencies

Budget Decision Unit(s): JIST
Strategic Goal(s) & Objective(s): Goal 4 – Enabling administration
Organizational Program: All JIST Programs
Programs Reduction: Positions 0 FTE 0 Dollars \$13,000

Description of Item

The Department is continually evaluating its programs and operations with the goal of achieving across-the-board economies of scale that result in increased efficiencies and cost savings. In FY 2012, the Department is focusing on areas in which savings can be achieved, which includes: printing, publications, travel, conferences, supplies, and general equipment. The allocated JIST share of the cost savings (offset) is (\$13,000).

Summary Justification

The Department is continually evaluating its programs and operations to identify across-the-board economies of scale that result cost savings by increasing efficiencies. In FY 2012, the Department is focusing on achieving cost savings in the areas of printing, publications, travel, conferences, supplies, and general equipment.

Impact on Performance

The implementation of administrative efficiencies cost savings will have little impact on performance.