U.S. Department of Justice

FY 2016 PERFORMANCE BUDGET
Congressional Justification

Justice Information Sharing Technology

Table of Contents

I. Overview

The FY 2016 Justice Information Sharing Technology (JIST) request is a total of $37,440,000 and 45 positions. JIST funds the Department of Justice's enterprise investments in information technology (IT). As a centralized fund under the control of the Department of Justice Chief Information Officer (DOJ CIO), it ensures that investments in IT systems, cyber security, and information sharing technology are well planned and aligned with the Department's overall IT strategy and enterprise architecture. CIO oversight of the Department's IT environments is critical, given the level of staff dependence on the IT infrastructure and security environments necessary to conduct legal, investigative, and administrative functions.

In FY 2016, the JIST appropriation will fund the DOJ CIO's continuing efforts to transform IT enterprise infrastructure and cyber security, the Office of the CIO's performance of responsibilities under the Clinger-Cohen Act of 1996 and more recently the Federal Information Technology Reform Act (FITARA; P.L. 113-291), and the coordination of the Department's responses to information requests from the Office of Management and Budget (OMB). JIST will fund investments in IT infrastructure, cyber security infrastructure and applications, and financial management that support the overall mission of the Department and contribute to the achievement of DOJ strategic goals. Electronic copies of the Department of Justice's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: http://www.justice.gov/02organizations/bpp.htm

DOJ will continue its savings reinvestment strategy, enacted in the FY 2014 budget, which will support Department-wide projects. As a result, up to $35,400,000 from components may be reprogrammed in FY 2016 to augment JIST resources to advance initiatives to transform IT enterprise infrastructure and cyber security.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
IT Transformation & Cyber Security (ITT&CS)	**Implement cost efficient, enterprise infrastructure for shared services, storage, hosting, networking, facilities, and support that can be leveraged across the Department; and continue to address new and emerging cyber security threats and implement advance intrusion detection and response capabilities to counter advanced persistent threats.**	**0**	**0**	**$4,074**	**18**
Digital Services	**Fund the development of a DOJ Digital Service team that will be responsible for driving the efficiency and effectiveness of the agency's highest-impact digital services, in coordination with the U.S. Digital Service (USDS) which was launched in August 2014.**	**0**	**0**	**$7,400**	**23**
Total		**0**	**0**	**$11,474**	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, [$25,842,000] *$37,440,000*, to remain available until expended: *Provided,* That the Attorney General may transfer up to $35,400,000 to this account, from funds made available to the Department of Justice in this Act for information technology, to remain available until expended, for enterprise-wide information technology initiatives: *Provided further*, That the transfer authority in the preceding proviso is in addition to any other transfer authority contained in this Act.

Analysis of Appropriations Language

New language is proposed to make the component funds transferred to JIST available as no-year funds as opposed to one year funds.

IV. Program Activity Justification

A. Justice Information Sharing Technology – (JIST)

JIST	Direct Pos.	Estimate FTE	Amount ($000)
2014 Enacted	59	52	25,842
2015 Enacted	45	45	25,842
Adjustments to Base			124
2016 Current Services	45	45	25,966
2016 Program Increases	0	0	11,474
2016 Request	45	45	37,440
Total Change 2015-2016	0	0	11,598

1. Program Description

JIST programs support the attainment of the Department's strategic goals by funding the Office of the CIO, which is responsible for the management and oversight of the Department's IT investments. The JIST appropriation supports the daily activities of the Department's agents, attorneys, analysts, and administrative staff, and funds the following programs to provide enterprise-wide, cost-effective IT infrastructure, cyber security applications, information sharing technologies, and a unified financial system.

a. IT Transformation and Cyber Security

The IT Transformation and Cyber Security (ITT&CS) Program is a long-term multiyear commitment that aims to transform IT by implementing shared IT infrastructure for the Department and shifting investments to the most efficient computing platforms, including shared services and next generation storage, hosting, networking, and facilities. The ITT&CS Program directly supports the Federal CIO's 25 Point Plan to Reform Federal IT Management and the Portfolio Stat (PSTAT) process, and aligns the Department's IT operations with the Federal Data Center Consolidation and Shared First Initiatives. Work on these initiatives began in FY 2012 and continues. The program consists of the following projects: cyber security, e-mail consolidation, data center consolidation, mobility and remote access, and desktops.

b. Public Key Infrastructure/HSPD-12

The Public Key Infrastructure (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; implementation of Federal ICAM across the network fabrics as identified in the National Strategy of Information Sharing and Safeguarding (NSISS) Priority Objective #4; program management and implementation support of Committee on National Security Systems (CNSS) initiatives;

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 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 greatly enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

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

c. Law Enforcement Information Sharing Program

The Law Enforcement Information Sharing Program (LEISP) represents a strategic approach to sharing data with other DOJ components, other federal agencies, and partners at the state, local, and tribal levels. 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 ensures compliance with applicable DOJ policies and memoranda that include, but are not limited to, data sharing, privacy, and technologies. LEISP-related database application systems 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.

d. Policy, Planning and Oversight

Office of the CIO - DOJ IT Management: JIST funds the Office of the CIO and the Policy & Planning Staff (PPS), which supports CIO management in complying with the Clinger-Cohen Act, the recent Federal Information Technology Reform Act (FITARA; P.L. 113-29), and other applicable laws, rules, and regulations for federal information resource management. The CIO has staff providing IT services in the Department's Working Capital Fund (WCF). As such, the OCIO is responsible for ensuring the delivery of services to customers, developing operating plans and rate structures, producing customer billings, and conducting the day-to-day management duties of the CIO. Within OCIO, PPS develops, implements, and oversees an

integrated approach for effectively and efficiently planning and managing DOJ's information technology resources, including the creation of operational budget plans for JIST and the WCF accounts, and the monitoring of the execution of funds against those plans throughout the fiscal year.

PPS staff is responsible for IT investment management including portfolio, program and project management. The investment management team 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 DIRB, the CIO Council, and the newly-established Department Program Review Board (DPRB), 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 (508), and other statutory requirements. In addition, PPS performs valuation management, which assesses and scores both value and risk to select and compare IT investments as part of the overall portfolio management.

Enterprise IT Architecture: Enterprise IT Architecture (EA) monitors and ensures compliance with OMB and Government Accountability Office (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 and performs EA governance/coordination across the Department; supports investment reviews DIRB and Information Technology Investment Management (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.

Chief Technology Officer: The Chief Technology Officer (CTO) identifies, evaluates, and facilitates the adoption of innovative new technologies that can result in significant increased value for the Department. The CTO goal is to create partnerships with DOJ components in the exploration of new technologies by progressing through requirements, concepts, design, component sponsorships and prototyping that eventually result in enhanced operational systems for use across the Department.

Enterprise Radio Communications (Program Office): The Department's CIO maintains oversight and strategic planning responsibility for DOJ's use of wireless spectrum and the related technologies that enable radio and other wireless communications. The JIST OCIO staff is responsible for performing the following functions for the Department's radio/wireless program:

- **Strategic Planning:** The Program Office staff works with the law enforcement components and represents the Department in the National Telecommunication and Information Administration (NTIA), White House, and other external entities on issues related to spectrum auctions, and the resulting impact on DOJ wireless operations. They advise the DOJ executive leadership on spectrum relocation and related wireless topics

including the Public Safety Broadband Network (PSBN). The staff also develops common wireless strategies for the Department, and coordinates with other Federal, State, Local and Tribal law enforcement partners on procurements, platform sharing and technical innovations.

- **Spectrum Management:** Serves as the Department representative to the NTIA and other federal agencies to coordinate all national and international radio frequency (RF) spectrum use on behalf of DOJ. This coordination includes evaluating thousands of spectrum use requests by other agencies for potential impact on DOJ operations, selecting appropriate frequencies for the domestic and foreign deployment of RF equipment during peacetime and emergency situations, as well as reviewing and updating the approximately 24,000 DOJ-wide plans for spectrum relocation as a result of spectrum auctions.
- **Oversight/Liaison/Coordination:** The staff provides oversight and investment guidance to the Department's wireless communications efforts, ensuring component equities are maintained and strategic objectives are met through the administration of the Wireless Communications Board (WCB).

e. Unified Financial Management Systems

The Unified Financial Management System (UFMS) is one of the Department's highest management priorities. Identified by the Department's Inspector General as "one of the most important challenges for the Department," the Department is implementing UFMS to replace legacy financial systems. This allows the Department to streamline and standardize business processes and procedures across all components as well as provide accurate, timely, and useful financial and procurement data to financial and program managers. In addition, UFMS assists the Department by improving financial management performance and aids in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security identified by the Department's Inspector General.

UFMS currently serves over 8,000 users from six DOJ organizations – Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the U.S. Marshals Service (USMS), Asset Forfeiture Program (AFP), Federal Bureau of Investigation (FBI), and the Federal Bureau of Prisons (BOP). The BOP uses only the acquisitions module at this point.

The final FBI implementation of UFMS went live nationwide as the financial system of record during the first quarter of FY 2014 with a total of 3,000 users. The FBI implementation was completed on schedule and within budget as with the other UFMS implementations. The UFMS Consolidation project, which was completed in March of FY 2014, consisted of two parts. Part 1 was a technical refresh of the Momentum application, which incorporates new federal data requirements and ensures compatibility with newer technology. Part 2 consisted of migrating sensitive but unclassified (SBU) customers to the newer version (UFMS 2.2) and transitioning DEA from UFMS 1.1 to the shared instance of UFMS, which will reduce operational costs and reduce risk. All SBU customers now operate on the same instance and codeline.

Going forward, the Department anticipates migrating the remaining users of the Financial Management Information System (FMIS) to the shared UFMS SBU environment. These consist of the Offices, Boards and Divisions (OBD), Grants organizations, and BOP financials. Initial planning for the migrations began in FY 2014 and two of the smaller OBDs will go live in FY 2016.

2. Performance Tables

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)											
DOJ Strategic Goal/Objective: 2.6 Protect the federal fisc and defend the interests of the United States											
RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2014		FY 2014		FY 2015		Current Services Adjustments and FY 2016 Program Change		FY 2016 Request	
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
		52	25,842 [9,900]	34	25,842 [20,301]	45	25,842 [4,636]	0	11,598 [-3,257]	45	37,440 [1,379]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2014		FY 2014		FY 2015		Current Services Adjustments and FY 2016 Program Change		FY 2015 Request	
Program Activity		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		52	25,842 [9,900]	34	25,842 [20,301]	45	25,842 [4,636]	0	11,598 [-3,257]	45	37,440 [1,379]
Performance Measure	Percentage of offenders booked through JABS	100%		100%		100%		N/A		100%	
Performance Measure	Maintain mainframe enterprise system availability for client organizations	99%		100%		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	85%		85%		85%		N/A		85%	

	PERFORMANCE MEASURE TABLE
	Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)
	DOJ Strategic Goal/Objective: 2.6 Protect the federal fisc and defend the interests of the United States

Performance Report and Performance Plan Targets		FY 2010	FY 2011	FY 2012	FY 2013	FY2014		FY 2015	FY 2016
		Actual	Actual	Actual	Actual	Target	**Actual**	Target	Target
Performance Measure	Percentage of offenders booked through JABS	98%	98%	99%	100%	100%	**100%**	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	99%	100%	100%	100%	99%	**100%**	99%	99%
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations	99%	99%	99%	99%	99%	**99%**	99%	99%
Performance Measure	Ensure IT systems are certified and accredited	100%	100%	100%	100%	100%	**100%**	100%	100%
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms	75%	90%	86%	85%	85%	**85%**	85%	85%

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

JIST programs support the Department's Strategic Goals by providing staff the enterprise IT infrastructure and security environments necessary to conduct legal, investigative, and administrative functions. Specifically, JIST supports Strategic Objective 2.6: *Protect the federal fisc and defend the interests of the United States*. The FY 2014 – FY 2018 Strategic Goals are:

- Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law.

- Strategic Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law.

- Strategic Goal 3: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels.

JIST provides resources so that the DOJ CIO can ensure that investments in IT infrastructure, cyber security infrastructure and applications, central solutions for commodity applications, secure communications, and information sharing technology are well planned and aligned with the Department's overall IT strategy and enterprise architecture. The Portfolio Stat (PSTAT) process, along with the commodity team structure and process, has identified investment initiatives to transform IT infrastructure which will drive efficiency and cost savings by centralizing the delivery of commodity IT services across the enterprise. The DOJ CIO focus is to advance these initiatives to transform IT enterprise structure and cyber security.

Major IT investments are periodically reviewed by the Department IT Investment Review Board (DIRB). The Deputy Attorney General chairs the board, and the DOJ CIO serves as vice chair. The DIRB includes the Assistant Attorney General for Administration, the Controller, and various Deputy CIOs.

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. The DIRB's principal functions in fulfilling its decision-making responsibilities are to:

- Ensure compliance with the Clinger-Cohen Act, the Federal Information Technology Reform 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;
- Annually review each component's IT investment portfolio, including business cases for new investments, to enable informed departmental IT portfolio decisions; and
- Develop and implement decision-making processes that are consistent with the purposes of the DIRB, as well as applicable congressional and OMB guidelines for selecting, monitoring, and evaluating information system investments.

In addition to the DIRB, the Deputy Attorney General in October 2014 established the Department Program Review Board (DPRB) made up of key Department level and component executives that will monitor and support major and high visibility IT projects and services, as well as evaluate IT budget enhancement requests, among other responsibilities. The DPRB will directly support the responsibilities of the DIRB, and its governance structure addresses key IT management tenets included in FITARA. The Department contributes to the Federal IT Dashboard that allows management to review various aspects of major initiatives. 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.

JIST provides resources for the executive secretariat functions of the DOJ CIO Council, the principal internal Department forum for addressing DOJ information resource management priorities, policies, and practices. JIST resources also operate the DOJ IT Intake process through which commodity IT purchases are reviewed against architectural, procurement, and vendor management standards.

In FY 2014 the Department established a Vendor Management Office (VMO), which provides centralized guidance and prioritization for the Department's decentralized strategic sourcing and commodity purchasing initiatives, utilizing the buying power of the entire Department. The VMO has a broad representation from procurement, legal services, IT and various business units that helps reduce costs and optimize value. The VMO will lead and assist in the analysis of procurement data and strategies; become the central repository of enterprise procurement vehicles; identify and communicate internal and industry best practices; provide expertise to assist in pricing analysis, procurement strategies and negotiations; and communicate with strategic external vendors, component partners and other government agencies.

b. Strategies to Accomplish Outcomes

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

- The **IT Transformation and Cyber Security Program** is a long-term multi-year commitment to transform the Department's IT enterprise infrastructure to centralize commodity IT services and cyber security. Work on this program began in FY 2012 and continues. The program currently consists of the following projects:

    1. **E-mail and Consolidation:** Departmental email consolidation is a long-term multi-year effort that began in FY 2012 with the consolidation of small email systems and the planning activities for a Department-wide email system. The initial phase of this project reduced the number of departmental non-classified email systems from 22 to 9 at its completion at the end of FY 2014. In addition, new and enhanced collaboration functionality will be introduced to participating components in FY 2015. The long-term goal of the program is to reduce the number of email systems as much as possible and provide enhanced enterprise messaging tools for the Department. The Department continues to evaluate and analyze non-classified email systems to minimize costs and maximize business value. In FY 2016, DOJ plans to consolidate additional components into an enterprise email solution model and is also exploring options to migrate Agency email systems to a Cloud Service Provider (CSP) in order to further gain efficiencies and strategic value.
    2. **Data Center Consolidation:** The goals of this project are to optimize and standardize IT infrastructure to improve operational efficiencies and agility; reduce the energy and real property footprint of DOJ's data center facilities; optimize the use of IT staff and labor resources supporting DOJ missions; and enhance DOJ's IT security posture. These goals will be achieved by reducing the number of DOJ data centers to three core data centers; leveraging cloud and commodity IT services; and migrating data processing to these locations and services with appropriate service agreements. DOJ has identified two FBI owned data centers and one DEA leased data center as facilities that will serve as DOJ Core Enterprise Facilities (CEF). The Department has closed 53 data centers since 2010, and plans to close 11additional data centers in FY 2015. Activities will continue in FY 2015 to close the Justice Data Center in Dallas by September 30, 2015. Planning activities for the transition and closure of the Justice Data Center in Rockville, MD will begin October 2016.
    3. **Cyber Security:** The primary focus of this project is the prevention and detection of insider and advanced cyber threats. The Department will continue to develop and implement enterprise trusted infrastructure and architecture to provide secure and resilient systems and networks, enhanced auditing, robust data management and access control that will safeguard Department information and ensure data availability.
    4. **Mobile Services:** The long term goal for mobile services is to enable employees to work outside of the office. In FY 2013/14, the Department conducted market research, collaborated with key components on research pilots, evaluated devices and device management systems, overhauled mobile contracts, implemented an enterprise mobile infrastructure platform for iOS and Android mobile phones, and began to set up broker services for service delivery. During this time, the Department renegotiated and consolidated over 40 mobile contracts into six

contracts – three of which are enterprise contracts that offer competitive rates for devices and carrier services, resulting in a cost savings for the Department of $4.1 million per year. The infrastructure platform includes remote access services that provide secure VPN access to DOJ data.

In FY 2015/16, the department will expand mobile phone services into a comprehensive mobile solution that will include mobile laptops, tablets, and other devices, with productivity tools and apps, to provide the user with increasingly secure remote access to DOJ data. Future capabilities may include PIV card access to replace the need for multiple passwords, enterprise Lync messaging capability for mobile devices, collaboration tools for remote meetings and file sharing, enterprise WiFi, as well as emerging technologies not yet known. On the service delivery side, planned activities include the acquisition of enterprise shared services for inventory management of mobile assets, mobile application management, mobile device management, mobile content management, and expanded support for the DOJ App Catalog.

5. **Desktops, Laptops, Printers and Helpdesk**: The short-term goal of this project is to understand DOJ metrics for Desktop, Laptops, Printers and Helpdesk. This includes all hardware, software and personnel costs, cost per user, cost per device, and cost per helpdesk ticket. This will help inform and improve strategic sourcing for desktops, laptops, and printers including establishing strategy, funding models, policy, and evaluations of architectures and solutions. Funding will be used in developing an enterprise/Virtual Desktop Infrastructure (VDI) strategy.

The FY 2016 JIST budget continues to include language to provide the Attorney General with additional transfer authority for reinvestment in DOJ enterprise-wide IT initiatives (up to $35.4 million). This reinvestment funding will provide for smart IT investments, and will allow the Department's CIO to pool purchasing power across the entire organization to drive down costs and improve service for Department-wide initiatives. The strategy strikes the right balance between empowering the component CIOs, while at the same time giving the Department CIO central authority over Enterprise IT investments.

- The **Public Key Infrastructure/Identity Management Program** develops the enterprise architecture standards for identity management and provides planning, training, operational support, and oversight of the HSPD-12 Personal Identification Verification card (PIVCard) deployment process for DOJ component employees and contractors. It also serves as the primary governing body for DOJ compliance and implementation of the Federal Identity, Credential, and Access Management (ICAM) infrastructure. The PKI program serves as DOJ's departmental issuer of PIVCards, which is a mandatory element of the Department's compliance with government standards that will allow cross-agency secure communications. The card and related processing will become integral for encrypting sensitive data, remote processing and telework, and automating workflows and authorizations (electronic signatures). Perhaps more significantly, the PKI program also engineers, implements, operates, and maintains critical technology infrastructure used by all DOJ components to allow PIVCard login to desktop and laptop computers, as well as mobile devices.

Additional technology infrastructure support provided to DOJ components by the program includes enabling technologies for identity data management, digital signing, application multi-factor authentication and more.

- The **Law Enforcement Information Sharing Program** (LEISP) represents a strategic approach to sharing data with other DOJ components, other federal agencies, and partners at the state, local, and tribal levels. LEISP-related database application systems 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 develops and promotes information sharing architectural standards and services for connecting ongoing projects within key DOJ components, under a common set of goals and objectives, and ensures compliance with applicable DOJ policies and memoranda that include, but are not limited to, data sharing, privacy, and technologies.

V. Program Increase

Item Name: **IT Transformation and Cyber Security**
Strategic Goal & Objective: Support Strategic Goals 1 - 3
Budget Decision Unit(s): JIST

Program Increase: Positions 0 FTE 0 Dollars $4,074,000

A. Description of Item

The increase of $4, 074,000 (all non-personnel) will continue to fund the IT Transformation and Cyber Security Program (ITT&CS) initiated in FY 2013 to:

- Implement the Federal CIO's 25 Point Plan to Reform Federal IT Management by implementing a cost-efficient enterprise IT infrastructure using infrastructure building blocks and IT systems that can be leveraged across the Department;
- Protect the Department against current and emerging cyber security threats by implementing security infrastructure to address insider threats and advanced persistent attack (APT) threats and upgrading the Department's trusted infrastructure.

The ITT&CS Program is a long-term multiyear effort to move the Department from its highly federated IT model to a more leveraged architecture and footprint and to protect the Department's networks from current and emerging cyber security threats.

1. Cyber Security

The Cyber Security and Insider Threat Program is aimed at protecting the Department against current and emerging cyber security threats by implementing security infrastructure to address insider threats and advanced persistent attack (APT) threats and upgrading the Department's trusted infrastructure.

It is a multiyear effort to protect the Department's networks from current and emerging cyber security threats. The cyber security threat directed toward the Department is not static; it is a dynamic threat with the scope, number, and complexity of cyber attacks changing and expanding. To effectively counter a changing and evolving cyber security threat, the Department must quickly address new threats and continually monitor, evaluate, and plan defenses against emerging threats that present near-term risk and potential loss.

The immediate cyber security risk facing the Department is insider threats and APT undertaken by large private/criminal organizations or nation state sponsored groups. The Department must continue work to consolidate and secure sensitive but unclassified (SBU) and classified networks to improve its overall security posture.

a. Insider Threat

The 2010 WikiLeaks incident, the 2012 Snowden incident, and other recent data leakage occurrences highlight the fact that insider threats pose one of the greatest risks to government information systems. Employees are trusted with sensitive and/or classified information and there is often little oversight or security governing that access. Implementing strong, flexible, and scalable measures to prevent insider attacks from succeeding is vital.

In February 2014, the Attorney General issued DOJ Order 0901 addressing Insider Threat. The Order establishes the Department's Insider Threat Program and the approach for identifying, deterring, and mitigating such threats. Of primary concern are the control and monitoring of removable media, insider threat behavior monitoring and detection, and prevention of data leaks on all sensitive and classified information systems.

To counter insider threats, the increase may be used to implement a defense plan and acquire and implement hardware infrastructure and software tools to monitor, detect, and respond to insider threats.

b. Advanced Persistent Threat (APT)

APT is a sophisticated and organized cyber-attack to access and steal information from compromised computers. These attacks are usually initiated by large private/criminal organizations or groups sponsored by nation states. The occurrence of APT attacks against the federal government, including the DOJ, is increasing.

APT intruders have malicious code (malware) that circumvents common safeguards such as anti-virus and intrusion detection systems and are capable of escalating their tools and techniques as our capability to respond improves. Therefore, the APT attacks present different challenges than addressing common computer security breaches.

New monitoring technologies such as host-based monitoring and signature detection technologies are critical to successfully identifying malicious activity that hides in routine network traffic or lies dormant until it is required to maintain access to the network. These technologies will allow the Justice Security Operations Center (JSOC) to identify malware often missed while monitoring networks. Without the implementation of these advanced technologies, DOJ will not know if it has been targeted by an APT which increases the risk of sensitive data loss and results in significant amounts of JSOC time wasted to conduct tactical remediation in an effort to understand the extent of a security compromise.

To effectively protect the networks and data, the Department's security architect and infrastructure must specifically take APTs into account. Next-generation software can provide advanced analytics of data which look for network or host based anomalies that will help uncover any attack or malware that may have slipped through the Department's security perimeter.

2. IT Transformation

The transformation of enterprise IT to a cost effective building block infrastructure is a multiyear program aimed toward implementing the shared IT infrastructure for the Department and shifting investment to the most-efficient computing platforms, including shared services and next generation storage, hosting, networking, and facilities. These infrastructure building blocks will facilitate modernizing and consolidating the Department's IT infrastructure by aligning the Department's IT operational requirements with the Federal Data Center Consolidation and Shared First Initiatives.

a. Data Center Consolidation

The Data Center Transformation Initiative (DCTI) is a multiyear effort to move the Department from its highly federated IT model to a more leveraged architecture and footprint. The Department has identified 3 Core Enterprise Facilities (CEFs) to provide data center services. The existing Justice Data Centers in Dallas (JDC-D) and Washington (JDC-W) will be closed in support of the Department's consolidation efforts. The JDC-D facility is planned for closure in September 2015 and JDC-W closure planning will commence in October 2015. Consolidation of core IT services into three facilities will significantly improve DOJ's data center efficiency and improve IT security. Current data centers were built using older power, heating and cooling models. The new data centers will incorporate third generation technologies to decrease cost and improve efficiency. Physical and information security will be improved through consolidation by reducing the number of people with physical access to equipment, placing it in more secure facilities, and consolidating equipment through virtualization. Virtualized hardware requires fewer machines to receive OS and security patches, thereby reducing possible vulnerabilities.

DOJ's core IT infrastructure is currently located at 57 remaining data centers, providing approximately 225,000 square feet of floor space for IT equipment, using 18 disparate component-run architectures. These inefficiencies arise in all aspects of the data center, from infrastructure, power consumption, labor, maintenance and physical and IT security. As a result, consolidation efforts must address the inefficiencies that exist as well as prepare the government to meet future mission demands.

The Federal Data Center Consolidation Initiative (FDCCI) mandates that the Department consolidates data centers and optimizes infrastructure to meet environmental, budget, and performance targets established for the federal enterprise. On May 11, 2012 OMB issued memo M-12-12 *Promoting Efficient Spending to Support Agency Operations* which provided practical guidance enforcing Presidential EO13589 *Promoting Efficient Spending*. While the mandate from OMB is clear in this area, DOJ leadership along with the CIO Council agrees with the need to consolidate infrastructure and has actively embraced the concept by closing 53 data centers to date and plans to close 11 and 9 additional data centers in FY 2015 and 2016, respectively. It has also begun to focus efforts on consolidating one of the Department's largest legacy data centers by the end of FY 2015. By shutting down and consolidating under-performing data centers and

optimizing our 3 Core Enterprise Facilities, we stand to save taxpayers millions of dollars and curb spending on underutilized infrastructure.

B. Justification

The ITT&CS Program is aimed toward implementing innovative and cost-efficient infrastructure models and enhancing the Department's security posture by implementing cyber security architecture and infrastructure to counter new and emerging cyber threats. Implementation of the infrastructure building-block model will reduce the cost of the Department's IT operations and facilitate further savings by consolidating data centers. It will strengthen the Department's capabilities to address new and emerging threats, ensure the protection of sensitive data, and facilitate the availability of networks and data so the Department's staff can securely conduct legal, investigative and administrative functions. The ITT&CS Program is a long-term multiyear effort that will significantly transform IT and cyber security infrastructures resulting in reduced operating costs and a more secure IT environment.

C. Impact on Performance

The Department's ability to achieve its strategic goals depends heavily on its IT and cyber security infrastructure to support its agents, attorneys, analysts, and administrative staff in conducting legal, investigative and administrative functions. The complexity of the mission, challenging business environment, and increasing need for collaboration are factors driving investments in IT.

To meet mission investigative and information sharing requirements, DOJ's agents, attorneys, and analysts are increasingly reliant on connectivity to the Internet, other DOJ components and multiple levels of government. The ITT&CS increase will allow the Department to address weaknesses in the current network and security architecture supporting the Department. This will not only improve the overall security of the network, but will improve the administration and monitoring of the network. Secure and resilient systems and networks will provide DOJ's agents, attorneys and analysts with the necessary IT tools to efficiently and effectively accomplish their missions.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
5	0	2	$8,749	5	0	4.5	$9,046	5	0	5	$9,129

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
	$0	0	$0	$0	$0
Total Personnel	$0	0	$ 0	$0	$0

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel (Software and Contractor Support)			$4,074	$2,100	$2,100

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	45	0	45	$725	$8,404	$9,129	$0	$0
Increases	0	0	0	$0	$4,074	$4,074	$2,100	$2,100
Grand Total	45	0	45	$725	$12,478	$13,203	$2,100	$2,100

Affected Crosscuts

The Cyber Security and National Security crosscuts will be affected by this request.

VI. Program Increase

Item Name: **Digital Services**
Strategic Goal & Objective: Support Strategic Goals 1 - 3
Budget Decision Unit(s): JIST

Program Increase: Positions 0 FTE 0 Dollars $7,400,000

A. Description of Item

The increase of $7,400,000 will fund the development of a DOJ Digital Service team in FY 2016. This Digital Service team will be responsible for driving the efficiency and effectiveness of the agency's highest-impact digital services. It will coordinate with the U.S. Digital Service (USDS) which was launched in August 2014. The USDS's main goal is to institutionalize the approach that salvaged and saved Healthcare.gov and apply it to government work to avoid similar incidents by setting standards, introducing a culture of technological accountability, and figuring out common technology patterns that can be replicated across agencies.

B. Justification

The success rate of government digital services is improved when agencies have digital service experts on staff with modern digital product design, software engineering, and product management skills. This funding will enable the Attorney General and his Deputy Secretary to build a DOJ Digital Service team that will focus on transforming the Department's digital services so they are easier to use and more cost-effective to build and maintain, with the greatest impact to citizens, communities, and organizations.

These digital service experts will bring private sector best practices in the disciplines of design, software engineering, and product management to bear on the Department's most important services. The positions will be term-limited, to encourage a continuous influx of up-to-date design and technology skills into the agency. The digital service experts will be recruited from among America's leading technology enterprises and startups, and will join with the Department's top technical and policy leaders to deliver meaningful and lasting improvements to services to citizens, communities, and organizations.

C. Impact on Performance

The Department's ability to achieve its strategic goals depends heavily on its IT capability to support its agents, attorneys, analysts, and administrative staff in conducting legal, investigative and administrative functions. In addition, IT facilitates public access to non-sensitive government data. The DOJ Digital Service team in cooperation with USDS is expected to improve digital services development and delivery.

The DOJ Digital Service team will be supported by the U.S. Digital Service which is "charged with removing barriers to exceptional Government service delivery and remaking the digital experiences that citizens and businesses have with their Government"[1] . The U.S. Digital Service will be a "centralized, world-class capability…made up of our country's brightest digital talent"[2]. The USDS was a pilot project in FY 2014 and formally launched in August 2014. Since standing up, this small OMB team has worked in collaboration with Federal agencies to implement cutting edge digital and technology practices on the Nation's highest impact programs, including the successful re-launch of HealthCare.gov in its second year, which led to millions of Americans receiving health coverage; the Veterans Benefits Management System; online visa applications, green card replacements and renewals; among others. In addition to their work on these high priority projects, this small team of tech experts has worked to establish best practices (as published in the U.S. Digital Services Playbook at playbook.cio.gov) and to recruit still more highly skilled digital service experts and engineers into government. The goal is to amplify the team's influence by setting standards, introducing a culture of technological accountability, and figuring out common technology patterns that can be replicated across agencies.

Funding

Base Funding

FY 2014 Enacted				FY 2015 Enacted				FY 2016 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
0	0	0	$0	0	0	0	$0	0	0	0	$0

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
	$0	0	$0	$0	$0
Total Personnel	$0	0	$ 0	$0	$0

Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2016 Request ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Total Non-Personnel			$7,400	$0	$0

[1] Federal CIO Steve VanRoekel's testimony before the Senate's Homeland Security Committee in May 2014
[2] Op.cit.

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2017 Net Annualization (change from 2016) ($000)	FY 2018 Net Annualization (change from 2017) ($000)
Current Services	0	0	0	$0	$0	$0	$0	$0
Increases	0	0	0	$0	$7,400	$7,400	$0	$0
Grand Total	0	0	0	$0	$7,400	$7,400	$0	$0