U.S. Department of Justice

FY 2018 PERFORMANCE BUDGET
Congressional Justification

Justice Information Sharing Technology

Table of Contents

I. Overview

The FY 2018 Justice Information Sharing Technology (JIST) request totals $30,941,000 and includes 34 authorized positions. JIST traditionally has funded the Department of Justice's enterprise investments in information technology (IT), and this submission seeks to continue along the path of IT Transformation moving the Office of the Chief Information Officer toward a service-broker management model.

As a centralized fund under the control of the Department of Justice Chief Information Officer (DOJ CIO), the JIST account ensures that investments in IT systems, cybersecurity, 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 2018, the JIST appropriation will fund the DOJ CIO's continuing efforts to transform IT enterprise infrastructure and cybersecurity. These efforts include resources for the Office of the CIO's responsibilities under the Clinger-Cohen Act of 1996, and more recently resources to perform financial management and reporting and IT program management responsibilities directed by the Federal Information Technology Acquisition Reform Act (FITARA; P.L. 113-291). JIST will fund investments in IT infrastructure, cybersecurity infrastructure and applications 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 internet address: http://www.justice.gov/02organizations/bpp.html.

DOJ will continue its savings reinvestment strategy, enacted in the FY 2014 budget, which will support Department-wide IT initiatives. As a result, up to $35,400,000 from Components may be reprogrammed in FY 2018 and will be available until expended to augment JIST resources to advance initiatives that transform IT enterprise infrastructure and cybersecurity across the Department.

II. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, $30,941,000 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

No substantive changes proposed.

General Provision Language

[Sec. 209.None of the funds made available under this title shall be obligated or expended for any new or enhanced information technology program having total estimated development costs in excess of $100,000,000, unless the Deputy Attorney General and the Department Investment Review Board certify to the Committees on Appropriations of the House of Representatives and the Senate that the information technology program has appropriate program management controls and contractor oversight mechanisms in place, and that the program is compatible with the enterprise architecture of the Department of Justice.]

Analysis of Appropriations Language

This provision is no longer required due to the recent IT management controls included in the FITARA legislation, which provides for an inclusive governance process that enables effective planning, budgeting and execution for IT investments at the Department's senior leadership levels.

III. Program Activity Justification

A. Justice Information Sharing Technology – (JIST)

JIST	Direct Pos.	Estimate FTE	Amount ($000)
2016 Enacted	45	45	31,000
2017 Continuing Resolution	45	45	31,000
Rescission – 0.1901% Adjustments to Base and Technical Adjustments			-59
2018 Current Services	34	34	30,941
2018 Request	34	34	30,941
Total Change 2017-2018	-11	-11	-59

1. Program Description

JIST-funded programs support progress toward 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 portfolio. The JIST appropriation supports the daily OCIO IT-related activities relied upon by the Department's agents, attorneys, analysts, and administrative staff, and funds the following programs: cybersecurity; enterprise-wide, cost-effective IT infrastructure; Digital Services, and information sharing technologies.

a. Cybersecurity (Cross Agency Priority Goal)

Enhancing cybersecurity remains a top priority for the Department and its leadership as DOJ supports a wide range of missions that include National Security, law enforcement, prosecution, and incarceration. For each of these critical missions, the systems that support them must be secured to protect the confidentiality of sensitive information, the availability of data and workflows crucial to mission execution, and the integrity of data guiding critical decision-making. DOJ's cybersecurity investments directly support the President's Cross Agency Priority (CAP) Goal for cybersecurity that remains a top initiative reflected in the Administration's FY 2018 budget guidance.

The Department of Justice's Cybersecurity Services Staff (CSS) currently provides enterprise-level strategic security management, policy development, technology enhancements and solutions, and monitoring capabilities across the enterprise. While CSS continues to improve these activities; service personnel, hardware, and software costs have consistently risen, workload for current responsibilities has increased, threats to our systems have sky rocketed, many enterprise cybersecurity tools have reached end of life, and CSS has taken on new missions (e.g., Supply Chain and Insider Threat Prevention). The confluence of these responsibilities creates a situation whereby CSS, while mature in many aspects of cybersecurity, cannot adequately address the requirements of today's dynamic threat environment without significant investments similar to levels in FY 2015 – 2017. The amounts requested in this budget address the oversight role of both

DOJ and CSS, but do not cover the Component-level network security management, which is funded through the Component's annual budget.

The major lines of operations within CSS include the Justice Security Operations Center; Identity, Credential, and Access Management (ICAM); Information Security Continuous Monitoring; and Insider Threat Prevention and Detection.

- **Justice Security Operations Center**

The Justice Security Operations Center (JSOC) provides 24x7 monitoring of the Department's internet gateways and incident response management. In its monitoring function, DOJ continues to add new systems and new technologies to DOJ networks that require modern protection with capabilities for combatting the latest attack technologies used by adversaries. Concurrent with the increasing tempo of cyber-attack activities, paradigm shifts in IT, such as cloud computing and ubiquitous mobility, are placing increased emphasis on cybersecurity outside the traditional enterprise boundary. As DOJ embraces these new technological frontiers, CSS must ensure that they can be adopted and deployed in a secure fashion that supports the DOJ and component missions, while safeguarding the Department's data.

The Department needs infrastructure investments to modernize how incident response is handled across our geographically-dispersed DOJ footprint, and adapt to the changing technological landscape associated with cloud and mobility. Much of the Department's significant cybersecurity investments occurred several years back. Today, the JSOC's effectiveness is stunted by aged infrastructure, some of which is past end-of-life and less supportable.

- **Identity, Credential, and Access Management (ICAM)/Strong Authentication (Including Public Key Infrastructure/HSPD-12)**

The role of the Identity, Credential, and Access Management (ICAM) program is to establish a trusted identity for every DOJ user along with the access controls necessary to ensure that the right user is accessing the right resources at the right time. This program provides the planning, training, operational support, and oversight of HSPD-12 Personal Identification Verification card (PIVCard) deployment, and operates the ongoing centralized system for DOJ component employees and contractors. Looking forward, this program will have to address the authentication of mobile users and devices, network devices such as routers, switches, and printers/scanners, those privileged users with increased access and ability, and the broadening scope of cloud technology.

The Department does not currently manage the issuance of digital certificates which act as "keys" to the systems. DOJ PIV certificates are currently issued through the GSA USAccess Program: http://www.gsa.gov/portal/category/27240. The Department seeks to complete the build out of the capability to centrally manage (i.e. issue, scan, secure, and revoke) all digital certificates required for use on DOJ systems. This capability will also provide system owners with an automated mechanism to obtain trusted certificates from a

central location. Without a trusted central certificate authority, the Department has no way of knowing where its keys are and who is using them. Should attackers leverage a stolen certificate, they potentially could have unfettered access to Department systems and remain hidden from current JSOC sensors. As more systems move to the cloud and encryption becomes pervasive within the DOJ network, the Department must ensure that system owners are using trusted certificates and have a mechanism in place for detection when these certificates may become compromised.

- **Information Security and Continuous Monitoring**

The Information Security Continuous Monitoring (ISCM) program brings together the security technology tools for continuous diagnostics, mitigation, and reporting with the personnel to support the Federal Information Security Modernization Act (FISMA) system security authorization and implementation of cyber internal controls across the DOJ components. The ISCM program leverages enterprise-wide solutions for automated asset management, configuration, and vulnerability management; tools for scanning networks and systems for anomalies; endpoint encryption for secure workstations and data in-transit; and dashboard reporting for executive awareness and risk-based decision-making in near real-time. ISCM policy analysts fuse this system control assessment data with vulnerability and incident data to provide continuous and dynamic visibility into security posture changes that impact risks to the Department's missions.

- **Insider Threat Program**

The DOJ Insider Threat Prevention and Detection Program (ITPDP) is responsible for protecting sensitive and classified information and resources from misuse, theft, unauthorized disclosure, or espionage by insiders. The DOJ Insider Threat Program was established under Executive Order 13587 directing Executive Branch departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs. The ITPDP is integrated with DOJ Security and Emergency Planning Staff (SEPS) efforts to implement Insider Threat and Security, Suitability, and Credentialing Reform (ITSCR) throughout the Department.

In order to achieve the intent of the Insider Threat Full Operating Capability Goal, DOJ must have the capacity to detect patterns and correlated indicators across multiple types of information (e.g., human resources, information assurance, security, and counterintelligence). Having this capacity can lead to preventing (or mitigating) threats and adverse risks to the security of the United States. Building on FY 2015 - 2017 cyber-related expenditures, FY 2018 JIST funding provides increased capabilities for Continuous Monitoring of user activity on Department IT systems and building a Department hub to centralize information on user activity. The ITPDP will also exchange data with the ITSCR to perform insider threat analysis and investigations. This investment will enable the Department to expand and improve its proactive behavior analysis and detection of suspicious activities in near real time, providing assurance that system users are performing valid work-related activities.

b. IT Transformation

The IT Transformation (ITT) 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 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 into FY 2018 and beyond. The program consists of the following projects: e-mail consolidation, data center consolidation, enterprise IT cybersecurity investments, and desktops.

c. Law Enforcement Information Sharing Program The Law Enforcement Information Sharing Program has been moved from JIST to WCF and is now in O&M status.

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, FITARA, and other applicable laws, rules, and regulations for federal information resource management. The CIO has staff providing IT services funded through 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 responsibilities of the OCIO. 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 plans for the JIST and WCF accounts, and monitoring the execution of funds against those plans.

- **CIO Role in the Budget Process**

  On May 5, 2016, DOJ signed Order 0903, which updated the Department's policies with respect to IT management. This update specifically accounts for provisions enacted in FITARA, and details the Department's CIO's role in IT budget planning and execution, including:

  - IT program reporting and review policy, processes, and procedures. Specific reporting instructions and detail are published for each budget planning cycle.

  - The authority and the Department CIO participation in budget planning, review, and approval. IT resource planning, reporting, and review instructions are included in the CFO's overall budget planning process instructions, which are published each year and are coordinated with the formal Spring Call budget formulation process.

- The Department CIO's participation in the agency level budget planning, review, and approval processes, as part of his responsibility to advise the Attorney General and other leaders on the use of IT to enhance mission accomplishment, process improvement, and ensure information security.

The Department CIO reviews and approves the resource plans for major IT investments as part of the IT capital planning process. The CIO endorses the agency budget request for FY 2018. CIO participation in budget planning, review, and approval for major IT programs is defined in agency budget planning guidance, policy, and process descriptions. The OCIO worked collaboratively with the Office of Management and Budget to secure approval of the Department's FITARA implementation plan.

PPS 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 Department IT Investment Review Board (DIRB), the CIO Council, and the Department Investment Review Council (DIRC). 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 reviews to examine planned IT acquisitions and procurements to ensure alignment with the Department's IT strategies, policies, and its enterprise road map.

e. Enterprise IT Architecture

Enterprise Architecture (EA) leverages component-based EA programs and IT Investment Management (ITIM) programs, to create a Federated EA. EA provides high-level guidance on architectural issues and provides a central point for aggregating and reporting on activities from across components. EA monitors and ensures compliance with OMB and Government Accountability Office (GAO) enterprise architecture requirements. EA participates in a wide range of IT planning, governance and oversight processes at the Departmental level, such as the ITIM and Capital Planning and Investment Control (CPIC) processes, as well as participating in review boards and IT planning Initiatives. This interaction allows OCIO to review IT investments for enterprise architecture alignment and to collect specific IT information during the ITIM process. EA documents the DOJ IT Portfolio within an enterprise architecture repository. The enterprise architecture repository contains information on all departmental systems and provides supporting information to Departmental Initiatives and maintains the Department's IT Asset Inventory in compliance with OMB Circular A-130. Additionally, EA represents the Department's components in cross-government EA forums and with oversight agencies, and assists DOJ IT planning and strategic efforts including, but not limited to, Information Sharing, Investment Review, and Open Data.

f. Chief Technology Officer

The Chief Technology Officer (CTO) identifies, evaluates, and facilitates the adoption of innovative new technologies that can result in significantly increased value for the Department. A key objective of the CTO 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 results in enhanced operational systems that support the mission and can be used across the Department.

g. Enterprise Radio Communications (Program Office)

The OCIO maintains oversight and strategic planning responsibility for DOJ's use of spectrum for tactical wireless and related technologies that enable radio and other wireless communications in support of DOJ's law enforcement and investigative missions. JIST-funded OCIO staff is responsible for performing the following functions for the Department's radio/wireless program:

- **Strategic Planning:** OCIO staff works with DOJ's law enforcement components and represents the Department with the National Telecommunication and Information Administration (NTIA), the White House, and other external entities on issues related to spectrum auctions, and the resulting impact to DOJ operations. Staff advises on spectrum relocation and related wireless topics, including the Public Safety Broadband Network (PSBN) and FirstNet. Staff also develops common wireless strategies for the Department, and coordinates procurements, platform sharing, and technical innovations.

- **Spectrum Management:** Staff serves as the Departmental representative to the NTIA and other federal agencies to coordinate all national and international radio frequency (RF) spectrum use on behalf of DOJ.

    - The coordination of spectrum use 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 22,000 DOJ-wide frequency assignments and reviewing plans for spectrum relocation as a result of spectrum auctions.
    - The staff will provide guidance and oversight for the procurement of spectrum dependent systems by obtaining certifications of spectrum support from NTIA, Department of Commerce. This process ensures that radio frequencies can be made available prior to the development or procurement of major radio spectrum-dependent systems required to meet mission/operational requirements. NTIA may also review the economic analyses of alternative systems/solutions at any point in the NTIA authorization processes.

- **Spectrum Relocation:** Staff works with leadership, DOJ Budget Staff, and interagency partners (OMB, NTIA) to effectively transition law enforcement wireless capabilities from auctioned radio spectrum to other spectrum bands. A key part of this effort is the Spectrum Relocation Office, which provides oversight of auction proceeds used to vacate spectrum and re-build affected wireless capabilities.

- **Oversight/Liaison/Coordination:** Staff provides oversight and investment guidance on the Department's wireless communications efforts, ensuring equities are maintained and that strategic objectives are met through the administration of the Wireless Communications Board (WCB).

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 2016		FY 2016(As of 3/31/16)		FY 2017		Current Services Adjustments and FY 2018 Program Change		FY 2018 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
		45	31,000 [9,892]	45	31,000 [44,315]	45	30,941 [25,367]	0	0 [-22,165]	34	30,941 [3,202]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2016		FY 2016		FY 2017		Current Services Adjustments and FY 2018 Program Change		FY 2018	
Program Activity		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		45	31,000 [9,892]	45	31,000 [44,315]	45	30,941 [25,367]	0	0 [-22,165]	34	30,941 [3,202]
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%		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	85%		89%		85%		N/A		85%	

2. Performance Tables

	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 2012	FY 2013	FY 2014	FY2015	FY 2016		FY 2017	FY 2018
		Actual	Actual	Actual	Actual	**Target**	Actual	Target	Target
Performance Measure	Percentage of offenders booked through JABS	99%	100%	100%	100%	100%	100%	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	100%	100%	100%	100%	99%	99%	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	86%	85%	85%	85%	85%	89%	85%	85%

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

JIST-funded programs support the Strategic Plan for Information Services and Technology (FY 2015 – 2018) that, at its core, seeks to advance, protect, and serve the mission. Programs funded through JIST also support the Department's Strategic Goals by providing enterprise IT infrastructure and security environments necessary to conduct national security, 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 –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.

The JIST account provides resources so that OCIO can ensure that investments in IT infrastructure, cybersecurity infrastructure and applications, central solutions for commodity applications, and information sharing technologies are well planned and aligned with the Department's overall IT strategy and enterprise architecture. 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 law enforcement infrastructure and cybersecurity requirements.

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 Department's Controller, and various IT executives representing key DOJ components.

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, FITARA, 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 investments are achieved;
- Ensure that 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 systems investments.

In addition to the DIRB, the Deputy Attorney General in October 2014 established the Department Investment Review Council (DIRC), which is 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 DIRC directly supports 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.

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 planned acquisitions 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 efforts. The VMO's Program Managers and Attorney Advisors bring together a wide range of experience and expertise, which has been instrumental in negotiating enterprise deals, facilitating the resolution of contractual disputes, coordinating, and consolidating component-led efforts and providing comprehensive management for JMD's Department-wide contracts. In order to stay current on new technology and industry best practices, the VMO maintains open and continuous communication with public and private technical and acquisition communities and disseminates findings in VMO-lead monthly meetings with cross-component participation. The VMO also drafts and revises IT acquisition policy and strategy and is currently creating a repository of samples, templates and guides for each step of the IT acquisition process.

b. Strategies to Accomplish Outcomes

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

- The Cybersecurity program is a long-term investment that has grown in importance over the past several years. Enhancing mission-focused cybersecurity has become a top priority for the President, DOJ, and its leadership. The program consists of four main focus areas:

    1. **Justice Security Operations Center (JSOC):** The 24x7 JSOC provides cyber defense capabilities at the Internet gateway of the Department's network. The JSOC will implement tools and employ resources to reduce time between intrusion detection and response through the following actions: 1) strengthen the network against external and internal threats; 2) expand forensic analysis and capability; and 3) automate incident response.

    2. **Identity, Credential, and Access Management (ICAM):** This program ensures that users are identified properly and granted access only to information resources necessary to perform their job. ICAM efforts will implement a DOJ certificate lifecycle management system, resulting in a more secure enterprise by reducing the opportunity for identity fraud and increasing the safety of both government information and personal privacy.

    3. **Information System Continuous Monitoring (ISCM):** ISCM will improve the visibility into the security health of the organization through two major initiatives: 1) supporting, monitoring, and reporting on system and network security hygiene, including mission essential systems and user activity; and 2) providing subject matter expertise to support DOJ components and organizations in their efforts to properly secure systems.

    4. **DOJ's Insider Threat Prevention and Detection Program:** The ITPDP will implement the tools to perform user activity monitoring and establish the Department's insider threat hub. As a result, the insider threat risks on sensitive and classified information systems will be reduced and the DOJ will have a capability to prevent, detect, and respond to insider threats

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

    1. Enterprise E-mail 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 the end of FY 2014. In addition, new and enhanced collaboration functionality was introduced to participating components during FY 2015. The long-term goal is to reduce the number of email systems and provide enhanced enterprise messaging tools for all Department users. In FY 2016, DOJ plans to consolidate additional components under an enterprise email solution Cloud Service Provider (CSP) model in order to further gain efficiencies and strategic value. The design, implementation, and migration to the cloud are projected to occur between FY 2017 - 2019.

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 72 data centers since 2010, including the Justice Data Center in Dallas which was shuttered in FY 2015. Planning activities to close 9 additional data centers by the end of FY 2017 and 9 more in FY 2018 are underway.

3. **Mobility Services:** The long term goal for mobile services is to enable employees to work outside of the office just as effectively as they would at their desk. With the dynamic nature of smartphone capabilities, the DOJ Mobile Services team was established in FY 2013 and collaborates across components on mobility initiatives to implement enterprise shared services. Key accomplishments to date include detailed security guidance for the major mobility platforms as well as the implementation of a shared mobile device management (MDM) platform which manages the mobile devices for 15 components. DOJ also initiated a mobile app program by converting Justice.gov to a mobile-friendly platform and released the first custom mobile app to the public to support the Office of Attorney Recruitment and Management.

   The Department will continue to expand mobility service with productivity tools and apps to provide users an enhanced experience with increasingly secure remote access to DOJ data. The DOJ App Catalog will be expanded to provide additional access to commercially available applications as well as new internally-developed apps. Other enhancements will focus on collaboration tools for remote meetings, enterprise file management for improved information sharing, Enterprise Wi-Fi, derived PIV integration to replace the need for multiple passwords, as well as emerging technologies.

4. **Enterprise Desktop**: The enterprise desktop area is converging with mobile devices, and the leading desktop vendors are rapidly introducing new laptop and

tablet solutions which can significantly enhance the user experience while at the office or working remotely. The key goals of this project are to provide a common user experience regardless of the device one is using, and also to expand the set of available device options in order to better fit the need of the user. Several components are planning JCON workstation refreshes for FY 2018 so the Enterprise Desktop team will continue to work closely with components to re-use these common solutions and standards across groups.

- **The Digital Transformation** team is responsible for driving the efficiency and effectiveness of the agency's highest-impact digital services. It will coordinate with U.S. Digital Service (USDS), which was launched in August 2014. The USDS' main goal is to institutionalize digital competencies and apply it to government work to avoid incidents, such as the challenges seen during the role-out of Healthcare.gov, by setting standards, introducing a culture of technological accountability, and assessing common technology patterns that can be replicated across agencies.

  The Department continues to engage the U.S. Digital Service, most recently facilitating the review of the FBI's National Instant Criminal Background Check System (NICS) and a discussion toward a decision point on the program's way forward. The Department has embraced the concept of the U.S. Digital Service (USDS) and continues to evaluate programs through its governance role assessing what, if any, information technology initiatives or programs may be served best by introducing a Digital Service Team. The current IT environment across the Department is focusing principally on securing deployed assets buffering them from cyber-attacks, and addressing high-risk legacy systems and networks, leaving little funding for true IT initiative development and modernization on which Digital Service teams might take an active participatory role.

  The Department coordinated with USDS leveraging the associated Schedule A hiring authority bringing in to the Department's OCIO, private sector expertise that is helping to progress the IT transformation effort underway within OCIO. These Information Technology Distinguished Fellows (IT Fellows) are being actively recruited to leverage their specific skill sets needed to truly transform the OCIO to a service broker model. In FY 2017, OCIO allocated vacancies and associated expenses to bring aboard IT Fellows, all of whom report directly to the Department's Chief Technology Officer. These are term positions that will come in and address critical risks and issues, much as in the same way as proffered under the USDS, but on IT initiatives not necessarily requiring rescue. In FY 2018, the OCIO will continue to devote position vacancies and resources to address critical risks and issues. The Department will continue closely coordinating with OMB and USDS, and through the IT governance structure, any IT programs requiring specific attention will be promptly assessed and USDS will be engaged thereafter, should the need arise.

- **Cyber-Space-** The DOJ will coordinate with Networking and Information Technology Research (NITRD) and Office of Science and Technology (OSTP) to drive research guided by the White House's "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program". With the perspective of the

Department's unique mission requirements, DOJ will perform research to understand the root cause of existing cybersecurity deficiencies; minimize future cybersecurity problems by developing the science of security; coordinate, collaborate, and integrate this research across the Government; and expedite the transition of cybersecurity research to practice.

- **Collaboration and Innovations with partnering agencies and private sector-** DOJ, with the FBI, will continue to work with industry, and partnering agencies, to learn and share strategies to provide insights into our critical mission needs. The Department of Justice will support the National Strategic Computing Initiative to maximize the benefits of High Performance Computing for economic competitiveness and scientific discovery. As investments in High Performance Computing has contributed substantially to national economic prosperity and rapidly accelerated scientific discovery, DOJ is committed to creating and deploying technology at the leading edge which advances our mission and spurs innovation.

- **Big Data-** As data is growing exponentially, High Performance Computing is the primary tools to spur insight, and perform big data analytics. Computing, storage, and high-speed networking coupled with analytics software will assist data scientists and mission owners throughout the department. These capabilities will advance many initiatives, including the Department's Automated Litigation Services, expediently analyzing images, and providing real-time intelligence for our law-enforcement – helping to ensure the safety of the American people.