U.S. Department of Justice

FY 2017 PERFORMANCE BUDGET
Congressional Justification

Justice Information Sharing Technology

Table of Contents

I. Overview

The FY 2017 Justice Information Sharing Technology (JIST) request totals $57,561,000 and includes 45 authorized positions. JIST traditionally has funded the Department of Justice's enterprise investments in information technology (IT). This FY 2017 submission also significantly enhances the OCIO's cybersecurity program. The existing environment of escalating cyberattacks, particularly against strategic government targets similar to the 2015 OPM attack, insider threats, and the need for continuous systems monitoring, especially on mission-essential systems, necessitates cyber-related investment enhancements. The sums requested for cybersecurity in this budget request represent an overall net increase to the FY 2017 JIST account, and builds on critical investments in cybersecurity executed in FY 2015 and planned for FY 2016.

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 2017, 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 at: 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 2017 and will be available until expended to augment JIST resources to advance initiatives that transform IT enterprise infrastructure and cybersecurity across the Department.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Cybersecurity	1. Justice Security Operations Center (JSOC) 2. Identity, Credential, and Access Management (ICAM) 3. Information Security Continuous Monitoring (ISCM) 4. Insider Threat Prevention and Detection Program (ITPDP)			$9,240 $6,600 $6,600 $4,000	21 24 27 30
Total				$26,440	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, $57,561,000 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 provide for an inclusive governance process that enables effective planning, budgeting and execution for IT investments at the Department's senior leadership levels.

IV. Program Activity Justification

A. Justice Information Sharing Technology – (JIST)

JIST	Direct Pos.	Estimate FTE	Amount ($000)
2015 Enacted	45	35	25,842
2016 President's Budget	45	45	31,000
Adjustments to Base			121
2017 Current Services	45	45	31,121
2017 Program Increases	0	0	26,440
2017 Request	45	45	57,561
Total Change 2016-2017	0	0	26,561

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 2017 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 beyond the current funding baseline. The enhancements requested in this budget address the oversight role of

both DOJ and CSS, but does 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 invest in building out 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 and planned FY 2016 cyber-related expenditures, FY 2017 JIST funding provides 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 initiatives to inform insider threat analysis and investigations. This investment will enable the Department to conduct 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 2017 and beyond. The program consists of the following projects: e-mail consolidation, data center consolidation, mobility and remote access, and desktops.

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-related database application systems enable state, local, and federal law enforcement agencies nationwide to collect, share, and analyze law enforcement information on criminal activities. 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. Most recently, the Department has committed its support and in FY 2016 will begin provisioning kiosks to participating Tribal law enforcement entities to enable critical information to be shared in an effort to combat crime committed on Tribal lands.

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 Federal Information Technology Acquisition Reform Act, 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 under FITARA**

  DOJ IRM Program Order 2880.1C and implementing instructions, including DOJ IT Governance Guide, and annual agency budget planning memoranda from the Attorney

General, Assistant Attorney General for Administration, and the Chief Information Officer define:

- 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 2017. CIO participation in budget planning, review, and approval for major IT programs is defined in agency budget planning guidance, policy, and process descriptions.

- **FITARA Implementation**

The Office of the CIO formed a Tiger Team composed of senior IT leaders and managers from across the Department to assess DOJ's alignment with the requirements outlined in OMB Memo M-15-14, Management and Oversight of Federal Information Technology, Attachment A, Common Baseline. The Tiger Team's findings were approved and submitted to OMB citing specific evidence of alignment with all but 5 elements of the Common Baseline.

The Tiger Team prepared and submitted for approval an implementation plan with these primary objectives:

1. Develop and implement policy, processes and procedures to meet the requirements outlined in the Common Baseline where the DOJ has not implemented the stated requirements.
2. Modify as necessary existing policy, processes and procedures to meet the requirements outlined in the Common Baseline where the DOJ has partially implemented the stated requirements.

Elements of this plan were to be completed and fully implemented by December 31, 2015 and include:

- CIO role on program governance boards.
- Shared acquisition and procurement responsibilities between CIO and SPE
- CIO review and approval of acquisition strategy and acquisition plan

- CIO approval of reprogramming
- CIO role in ongoing bureau CIOs' evaluations

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. The Office of Management and Budget has formally approved the Department's FITARA implementation plan.

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).

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 2015		FY 2015 (As of 9/30/15)		FY 2016		Current Services Adjustments and FY 2017 Program Change		FY 2017 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	25,842 [4,636]	35	25,842 [35,570]	45	31,000 [9,892]	0	26,561 [178]	45	57,561 [10,070]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2015		FY 2015		FY 2016		Current Services Adjustments and FY 2017 Program Change		FY 2017	
Program Activity		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		45	25,842 [4,636]	35	25,842 [35,570]	45	31,000 [9,892]	0	26,561 178]	45	57,561 [10,070]
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%		91%		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 2011	FY 2012	FY 2013	FY 2014	FY2015		FY 2016	FY 2017
		Actual	Actual	Actual	Actual	Target	**Actual**	Target	Target
Performance Measure	Percentage of offenders booked through JABS	98%	99%	100%	100%	100%	100%	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	100%	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	90%	86%	85%	85%	85%	91%	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 (FYs 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 – 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.

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. 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 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, the Federal Information Technology Acquisition 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 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, notably during FY 2015. 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 in 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 66 data centers since 2010, and the Justice Data Center in Dallas was shuttered during FY 2015. Planning activities to close 8 additional data centers by the end of FY 2016 and 7 more in FY 2017 are underway.

3. **Mobile 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.

   Planned for FYs 2016 and 2017, the Department will 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 FYs 2016 and 2017 so the Enterprise Desktop team will continue to work closely with components to re-use these common solutions and standards across groups.

- **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.

- **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's 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.

  We have coordinated with the U.S. Digital Service 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 FY16 we are allocating vacancies and associated expenses to bring aboard IT Fellows, all of whom will 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 U.S. Digital Service, but on IT initiatives not necessarily requiring rescue, which is the true value of USDS. In FY17, 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.

V. Program Increases by Item

Item Name: **Justice Security Operations Center (JSOC)**

Strategic Goal: Supports Strategic Goal 1-3
Budget Decision Unit(s): JIST
Organizational Program: JMD/OCIO / Cybersecurity Services Staff (CSS)

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $9,240,000

Description of Item

The JSOC is a 24x7 operation that provides comprehensive cyber incident detection, monitoring, and response management services for protecting the DOJ's computer networks. The adversaries attempting to harm the DOJ networks, systems, and employees are increasing in numbers, intent, and sophistication, and the JSOC is the central coordination point for the entire Department's cyber defense activities.

One of the major aspects of JSOC operations is the hunt for the Advanced Persistent Threat; APTs are a sophisticated and organized cyber-espionage activity with the mission of accessing and stealing information from compromised computers (the 2015 OPM cyberattack is an example of APT). In the event of hostilities, APT espionage activity can rapidly turn destructive (Sony) and cripple every aspect of DOJ's mission. The JSOC currently tracks over 1,000 possible APT events every year. At present time, much of the JSOC's APT defense capabilities are manually executed and lack modern capabilities. Compounding the issue is the rapid dissolution of the Department's network boundaries due to "cloud first" implementations.

Another major part of JSOC is Incident Response (IR), Analysis, and Investigation support. Since 2011, DOJ has consistently experienced around 7,000 cybersecurity incidents per year. JSOC uses a variety of technologies to perform advanced analysis of systems, network traffic, and malicious software. This includes detection and elimination of events such as covert communication channels, malicious software (Trojans, root kits, viruses, worms, etc.), and unauthorized network devices.

The $9.2 million enhancement request will allow DOJ to consolidate SOC operations using modern tools to combat adversaries seeking to harm the Department through cyber intrusion.

Justification

While cloud capabilities offer the Department flexible cost effective platforms, new security infrastructure capable of monitoring those platforms must be put in-place or DOJ risks having a significant breach of its systems. To combat APT where the DOJ's data resides, the JSOC must consolidate and leverage new monitoring, analysis, and response technologies in order to quickly and effectively respond to malicious activity that hides in routine network traffic or lies dormant until it is required to gain access to the data. Centralizing advanced capabilities will provide the JSOC with the ability to leverage cyber intelligence across the Department to locate and identify traces of APT. The JSOC has numerous sources of cyber intelligence; however, it is only able to

leverage a small fraction of the information and the fusion process is manual and does not permit the application of intelligence indicators across the Enterprise.

The Department of Justice is especially attractive to cyber attackers and intrusions because of its law enforcement, litigation, incarceration, civil protection, and national security missions, and is under a constant barrage of seemingly malicious attempts to access the DOJ systems and networks. The investment in the JSOC program will allow the Department to analyze the relevant data sources to be more agile in its detection and response to cyber threats and attacks. Secure and resilient systems and networks will provide DOJ's agents, attorneys, and analysts with the necessary fully-functioning, secure IT tools to accomplish the DOJ mission. Additionally, FY 2017 investments will fund the recurring costs of JSOC investments in FY 2015 and planned for FY 2016.

Impact on Performance

Cybersecurity is a crucial aspect of business in the twenty-first century. Cyber-breaches are increasing in both number and severity, as witnessed with the attack on the Office of Personnel Management (OPM) in June 2015, and the frequency of reports of high-profile intrusions and attacks across the public and private sector serve as reminders of the serious threats that exist. Few, if any, organization missions can be executed without the support of information technology (IT) systems. Those systems must be secured to protect sensitive data, the availability of data and workflows crucial to mission execution, and the integrity of data that guides critical decision-making.

Without modernizing the technology, the evolving and dangerous Advanced Persistent Threats will not be adequately addressed. Today, many of the APT defensive activities are manually executed by the JSOC team; however, with the sophistication of the threats increasing, automating and installing the newest technologies is vital to protecting the DOJ mission.

Additionally, the security IT infrastructure was not originally designed for the tremendous volume of today's system activity, so if an OPM-type incident was to occur, the aged infrastructure would preclude DOJ from conducting effective forensic analysis and incident response/containment, i.e., the Department would be drastically impacted and the ability to understand the extent of the damage would be minimal. As foreboding as that sounds, it pales in comparison to the impact of a Sony style destructive attack—every Departmental mission would be crippled and the Department would be unable to perform even its most basic functions.

Funding

FY 2015 Enacted				FY 2016 President's Budget				FY 2017 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
3	0	3	$492	3	0	3	$525	5	0	5	$875

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2016) ($000)	FY 2019 Net Annualization (change from 2017) ($000)
		0	$0	$0	$0
Total Personnel		0	$0	$0	$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Total Non-Personnel (Hardware, Software, Contractor Support)			$9,240	$3,200	$0

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	6	0	5	$875	$0	$875	$0	$0
Increases	0	0		$0	$9,240	$9,240	$3,200	0
Grand Total	5	0	5	$875	$9,240	$10,115	$3,200	$0

Affected Crosscuts

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

V. Program Increases by Item

Item Name:	**Identity, Credential, and Access Management (ICAM) (including Classified)**
Strategic Goal:	Supports Strategic Goal 1-3
Budget Decision Unit(s):	JIST
Organizational Program:	JMD/OCIO / Cybersecurity Services Staff (CSS)

Program Increase: Positions 0 Agt/Atty FTE 0 Dollars $6,600,000

Description of Item

The purpose 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.

Over the past several years, the Department has focused on issuing PIVCard/Smart Card credentials to eligible DOJ employees and contractors for access to unclassified and classified networks. The PIVCard is the government's solution for multi-factor authentication of personnel for system and facility access. To date, credentials have been issued to 94% of unclassified users and 95% of classified users. The current emphasis is on accelerating the mandatory use of these credentials for access to facilities and networks (currently 44% on unclassified networks, and 52% on classified networks), and applications (currently 18% on unclassified applications and 15% of classified applications).

The $6.6 million enhancement request is for an Enterprise Identity Management Solution that will issue, scan, secure, and revoke personal identity verification (PIV) card certificates based on HSPD-12 standards.

Justification

In order to take advantage of the investment in PIV, DOJ must move to an Enterprise identity management solution. This solution will permit internal applications, data center applications, and cloud-based systems to utilize PIV authentication. The solution will also permit the automated streamlining of user provisioning/de-provisioning. This will assist the Department by ensuring only those users with an authorized and valid PIV card are able to access Department systems wherever they may be located and there is one central location to disable user's access once they have left the Department.

The Department also requests funding to build out a Department managed PKI management system. PKI certificates are used by DOJ systems to secure network transmissions. As the Department moves more systems to the cloud, these systems rely on PKI to secure, encrypt, and enforce trust among entities. Moving to a Department managed PKI management group, the Department knows where its keys are stored and who is using them. This allows the JSOC to monitor encrypted streams for signs of malicious activity. With unmanaged keys, the JSOC cannot distinguish normal network traffic from that which may be malicious or harmful.

The key business drivers for the DOJ ICAM have been identified as the following:

- Transition from user name and password to multi-factor authentication to increase security by requiring a physical asset combined with a passcode, which limits the possibility of a hacker acquiring both. This correlates directly to a reduction in identity theft, data breaches, and trust violations. Specifically, ICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.
- Improved interoperability and trust, specifically between agencies using their PIV credentials. The credential is a trusted indicator of identity shared across the government.
- Centralized management of certificates ensures security of internal and cloud based systems, facilitates easier issuance and control of certificates.
- Large number of classified systems under management increases the need for multi-factor authentication.
- Limiting the types of credentials requiring oversight and management will bring efficiency and cost savings.
- Compliance with federal guidelines (e.g., FICAM Roadmap and FICAM on Secret Fabric Planning, HSPD-12, OMB M-11-11, EO 13587, CNSSD-506, and CNSSD-507) and the Cybersecurity CAP goals.

Impact on Performance

Identity, Credential, and Access Management is a crucial component of both facility and information systems security. Systems and applications need to be updated to allow for this multi-factor authentication effort, per the HSPD-12 requirements, to prevent unauthorized individuals from accessing DOJ information systems and facilities. Once implemented, these requested enhancements will align unclassified and classified ICAM initiatives, and allow the Department to not only become compliant with federal mandates, but also to enhance the user experience, permit improved access to systems and facilities, and facilitate greater interoperability between Federal organizations. Without this investment, the program will continue to struggle to meet the federal mandates, leave data and systems exposed to cyber threats through unmanaged keys, and be unable to keep up with authenticating users in mobile and cloud environments.

Funding

FY 2015 Enacted				FY 2016 President's Budget				FY 2017 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
0	0	0	$3,948	0	0	0	$4,114	0	0	0	$3,114

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
	$0	0	$0	$0	$0
Total Personnel		0	$0	$0	$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2016) ($000)	FY 2019 Net Annualization (change from 2017) ($000)
Total Non-Personnel (Hardware, Software, Contractor Support)			$6,600	2,300	

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total FY17 ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	0	0	0	$0	$3,114	$3,114	$0	$0
Increases	0	0	0	$0	$6,600	$6,600	$2,300	$0
Grand Total	0	0	0	$	$9,714	$9,714	$2,300	$0

Affected Crosscuts

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

V. Program Increases by Item

Item Name:	**Information Security Continuous Monitoring (ISCM)**
Strategic Goal:	Supports Strategic Goal 1-3
Budget Decision Unit(s):	JIST
Organizational Program:	JMD/OCIO / Cybersecurity Services Staff (CSS)

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $6,600,000

Description of Item

Funding in support of this program primarily comes from the WCF, with a nominal sum of JIST resources for government personnel. The program consists of two major parts: (1) supporting, monitoring, and reporting on system and network security health; and (2) providing personnel to support DOJ components and organizations in their efforts to properly secure their systems.

The Department has in-place a continuous monitoring program for enterprise-wide solutions to automate asset management, configuration, and vulnerability management; scan networks and systems for anomalies; encrypt workstations and data in-transit; and produce dashboard reports for executive awareness and risk-based decision-making.

ISCM Policy Analysts work with components to develop and facilitate awareness and understanding of IT security requirements. These Policy Analysts work directly with their respective component customers as their systems move through the certification and accreditation approvals and into operational environments.

The program increase of $6.6 million is for enhanced monitoring capabilities that index and analyzes additional IT information for use by components and for monitoring privileged accounts and user activity. It also includes recurring costs from planned cyber requirements in FY 2015 and FY 2016.

Justification

To meet ever-changing cyber threats and become the highly effective cybersecurity program DOJ needs, ISCM needs to evolve in the following ways:

- Acquire technologies that map network device configurations and potential attack paths that our adversaries could exploit. Enhance monitoring of privileged user accounts and user activity and expand the asset management capabilities beyond desktops and laptops to network devices (e.g., switches, routers) and mobile devices (e.g., tablets, smartphones).

- Obtain contractor support to incorporate additional threat and configuration feeds, build more detailed reporting and alerts, and automate certification and accreditation activities. Also, this investment will broaden the scope of the cybersecurity reporting to include not only IT system data, but also personnel/HR, financial, case management, and other data sources to enhance leadership's cybersecurity decision-making ability.

- Obtain contractor personnel to enhance the customer-centric Policy Analyst program with a broader scope of responsibility for the Federal Information System Management Act (FISMA) compliance, General Accounting Office Federal Information System Control Audit Manual (FISCAM) guidance, Audit Liaison, and Information System Security Officer (ISSO) for their component's customers.

While the asset management applications provide insight into the security posture of the enterprise and present the details in an easily digestible package for managerial risk-based decision-making, they provide only a partial view of the environment. Broadening the scope of systems being monitored and adding more data points and feeds would provide a more comprehensive view of the DOJ cybersecurity posture, IT environment, and potential weaknesses, thereby providing increased confidence to make enterprise-wide risk-based decisions. The ISCM program is also charged with incorporating and extracting value from the DHS Continuous Diagnostics and Mitigation program. The CDM program has provided specific visibility and gap fills for security areas. The program tools have been provided by DHS for a three-year period, and in FY 2017, DOJ must assume the operations and maintenance costs previously paid by DHS; $1,200,000.

Impact on Performance

The cyber threat landscape has evolved as technologies, capabilities, and incentives have changed. The threat actors have better equipment, better training, and more motivation to do the Department harm. The ability to monitor and protect DOJ's mission, to include networks, databases, end points, and applications is vital for a fully effective cybersecurity program to succeed.

To meet ever-changing cyber threats and become the highly effective cybersecurity program the Department needs, ISCM must invest to provide the following services:

- Increase coverage of indexing to include all users, traffic, and devices and provide analysis of all indexed data. This solution enables components to monitor network activity with sophisticated analytical techniques to enhance accountability, identify security threats, and investigate operational anomalies.

- Enhance reporting tools for executive cyber security decision making by including and correlating personnel/HR, financial, case management, and other data sources.

The ISCM program is integral in addressing cybercrime as a top DOJ Priority, particularly in the areas of deterrence, detection, and protection, as the program seeks to protect all electronic assets across the entire Department. Leveraging Policy Analysts and new technological advances, we will broaden our current approach for monitoring our security baseline to include new systems and data. With additional funding we will be able to incorporate a wide variety of new data, transform it into decision-making information, and use our Policy Analysts to institutionalize it throughout DOJ.

Funding

Base Funding

FY 2015 Enacted				FY 2016 President's Budget				FY 2017 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
1	0	1	$164	1	0	1	$175	1	0	1	$175

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
	$0	0	$0	$0	$0
Total Personnel		0	$0	$0	$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Total Non-Personnel (Hardware, software, contractor support)			$6,600	$2300	$0

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	FY17 Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	1	0	1	$175	$0	$175	$0	$0
Increases	0	0	0	$0	$6,600	$6,600	$2,300	$0
Grand Total	1	0	1	$175	$6,600	$6,775	$2,300	$0

Affected Crosscuts

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

V. Program Increases by Item

Item Name:	**Insider Threat Prevention and Detection Program (ITPDP)**
Strategic Goal:	Supports Strategic Goal 1-3
Budget Decision Unit(s):	JIST
Organizational Program:	JMD/OCIO / Cybersecurity Services Staff (CSS)

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $4,000,000

Description of Item

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 Assistant Attorney General for Administration is designated as DOJ's Senior Department Official (SDO) with the authority to provide and delegate responsibility for management, accountability, and oversight of the DOJ ITPDP as outlined in DOJ Order 0901, *Insider Threat*. Clearly communicated roles and responsibilities among the components are critical to preventing and detecting insider threats and meeting national insider threat requirements.

To meet the program goals, the DOJ ITPDP performs five primary functions:

- Collect and integrate user activity data from various offices and sources
- Analyze collected data to identify indicators of insider threats
- Track insider threat matters brought to the attention of the DOJ ITPDP
- Make the appropriate law enforcement or administrative referrals when possible insider threat activity is discovered
- Educate all employees and contractors on insider threat

The program remains immature in its development and DOJ does not yet have full capability in any of the five functions above.

The enhancement request of $4.0 million is for acquisition and integration of a user activity monitoring platform and building of a Department hub to centralize information on user activity for Insider Threat analysis.

Justification

To mature the program to appropriate levels, resources must be dedicated to advance and enhance each of the five points above.

- Employ the technology and personnel to connect and monitor user activity across the entire enterprise

- Implement the systems and train the personnel to conduct analysis on the data to identify anomalies in behavior and indicators of potential insider threat activities
- Train personnel on managing the process of pursuing insiders from identification through investigation
- Develop and distribute a more advanced insider threat awareness training, and establish a baseline training program for resources working on the ITPDP

Insider threat is a major attack vector that can produce the most damage for an organization. In examining the most infamous, government data breaches in recent memory, all were perpetrated by insiders: Robert Hansen at the FBI sold hundreds of classified documents to the Russians for profit; Edward Snowden "liberated" thousands of records and documents from the NSA to expose perceived wrong-doing; and Bradley Manning provided WikiLeaks with hundreds of thousands of classified files "to open America's eyes" to the conflicts in Iraq and Afghanistan.

Given DOJ's critical and sensitive mission, it is imperative to strengthen DOJ's ability to prevent and detect insider threats in real time. The current program is nascent in its capabilities and needs to grow the technical foundation and analytic competencies to perform the primary insider threat program functions. To be comprehensive this needs to be accomplished across both classified and unclassified systems because focusing on only either one addresses just half of the possible problems.

DOJ is especially attractive to insiders because of its national security, law enforcement, litigation, incarceration, and civil protection missions. Establishing a technically-capable and independent program is necessary to identify and pursue insider threats in these critical mission areas.

Impact on Performance

This investment will be used to build an insider threat solution that enables us to know where critical information is, who is accessing it, and if the access is authorized. The solution will enable the proactive detection of patterns and correlated indicators across multiple types of information (e.g. human resources, information assurance, security classification, and counterintelligence) that can lead to the prevention or mitigation of harm to the security of the United States. Further, this investment centralizes data sources and processes into a DOJ insider threat hub for fast and comprehensive views of diverse data streams. Once the DOJ insider threat program is built, DOJ will have insight into the anomalous activity that can indicate insider threats, and the processes in place to gather the data and pursue the inside threat actors to a proper conclusion.

Without these additional resources, the tools will not be available to perform user activity monitoring or behavioral analysis, nor will the insider threat analysis be in place to perform the necessary functions. As a result, the insider threat risks to sensitive and classified information systems will not be sufficiently addressed and the DOJ efforts to prevent, detect, and respond to insider threats will remain inadequate.

The Insider Threat Prevention and Detection Program is integral to supporting the Funding Priority of Cybercrime in the areas of Deterrence, Detection, and Protection, and the program seeks to protect the electronic assets and reputation of the entire Department.

Funding

Base Funding

FY 2015 Enacted				FY 2016 President's Budget				FY 2017 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
1	0	1	0	1	0	1	$175	1	0	1	$175

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2016) ($000)	FY 2019 Net Annualization (change from 2017) ($000)
	$0	0	$0	$0	$0
Total Personnel		0	$0	$0	$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2017 Request ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Total Non-Personnel (Hardware, Software, Contractor Support)			$4,000	$1,400	$0

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2018 Net Annualization (change from 2017) ($000)	FY 2019 Net Annualization (change from 2018) ($000)
Current Services	1	0	1	$175	$0	$175	$0	$0
Increases	0	0	0	$0	$4,000	$4,000	$1,400	$0
Grand Total	1	0	1	$175	$4,000	$4,175	$1,400	$0

Affected Crosscuts

The Cybersecurity and National Security crosscuts will be affected by this request