

U.S. Department of Justice

FY 2019 PERFORMANCE BUDGET

Congressional Justification

Justice Information Sharing Technology

Table of Contents

I. Overview	1
II. Summary of Program Changes	2
III. Appropriations Language and Analysis of Appropriations Language	3
IV. Program Activity Justification.....	4
A. Justice Information Sharing Technology – (JIST)	4
1. Program Description	4
2. Performance Tables (To be provided at a later date)	
3. Performance, Resources, and Strategies (To be provided at a later date)	
V. Program Increases by Item	11
VI. Exhibits.....	13
A. Organizational Chart (Not Applicable)	
B. Summary of Requirements	
C. FY 2019 Program Increases/Offsets by Decision Unit	
D. Resources by DOJ Strategic Goal/Objective (To be provided at a later date)	
E. Justification for Technical and Base Adjustments	
F. Crosswalk of 2017 Availability	
G. Crosswalk of 2018 Availability	
H. Summary of Reimbursable Resources	
I. Detail of Permanent Positions by Category	
J. Financial Analysis of Program Changes	
K. Summary of Requirements by Object Class	
L. Summary of Requirements by Grade (Not Applicable)	
M. Senior Executive Service Reporting (Applies only to DEA and FBI) (Not Applicable)	

I. Overview

The FY 2019 Justice Information Sharing Technology (JIST) request totals \$31,713,000 and includes 33 authorized positions. JIST funds the Department of Justice's enterprise investments in information technology (IT). This submission continues IT Transformation by 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, coordinated among DOJ components and aligned with the Department's overall IT strategy and enterprise architecture. CIO oversight of the Department's IT environment is critical given the level of staff dependence on the IT infrastructure and cybersecurity posture necessary to conduct legal, investigative, and administrative functions.

In FY 2019, 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 the more recent 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's 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 may be transferred by the Attorney General from DOJ components IT budgets in FY 2019 and 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	Continuous Diagnostics and Mitigation (CDM)	0	0	\$772	11
Total		0	0	\$772	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, \$31,713,000 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 control provisions 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.

IV. Program Activity Justification

A. Justice Information Sharing Technology – (JIST)

JIST	Direct Pos.	Estimate FTE	Amount (\$000)
2017 Enacted	37	37	31,000
2018 Annualized CR	34	34	30,789
Adjustments to Base			152
Adjustments to Base – 2% Reduction			0
2019 Current Services	33	33	30,941
2019 Program Increase	0	0	772
2019 Request	33	33	31,713
Total Change 2018-2019	0	0	772

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

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 investigations, prosecution, and incarceration. For each of these critical missions, the systems that support them must be secured to protect the 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 remain a top initiative as reflected in the Administration’s FY 2019 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. 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, notably Supply Chain Risk Management and Insider Threat Prevention. The confluence of these responsibilities creates a situation whereby CSS, while mature in many aspects of cybersecurity, cannot fully and adequately address the requirements of today’s dynamic threat environment without continued investments similar to levels prioritized going back to FY 2015. The amounts requested in this budget address the cyber tool investments but Component-level network security management, are funded through individual Component’s annual budgets.

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

Justice Security Operations Center

The 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 protection with capabilities for combatting the latest attack technologies used by adversaries. The increasing frequency of cyber-attack activities and the paradigm shifts in IT, such as cloud computing and ubiquitous mobility, are placing an increased emphasis on cybersecurity outside the traditional enterprise boundary. As DOJ embraces these new technological frontiers, CSS must ensure they can be adopted and deployed in a secure fashion supporting the DOJ and component missions, while safeguarding data.

The Department needs to continually invest in infrastructure modernization across DOJ's geographically-dispersed footprint, and adapt to the changing technological landscape associated with cloud and mobility or else face an environment where effectiveness is challenged by aged and unsupported infrastructure.

Identity, Credential, and Access Management (ICAM)

The role of the 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 services across the three ICAM foundational areas: 1) Identity, 2) Credential, and 3) Access Management. Looking forward, the ICAM program will be enhanced in the following ways:

- Identity Services – Enhancement and expansion of the Identity and Access Management (IAM) and Privileged Account Manager (PAM) solutions. This initiative builds on the implementations in FY 2017 to mature the IAM solution and complete the deployment of the PAM across the Department, and integrate JMD systems to leverage the IAM capability. JMD will work with Components to determine the best phased order of implementation and support the rollout based on lessons learned from the initial implementation. Successful implementation allows for comprehensive and secure management of the identity lifecycle of all DOJ users and devices.
- Credential Services – The Personal Identity Verification (PIV) card is the cornerstone credential of DOJ serving as the primary two-factor authentication token for logical access to DOJ networks, applications, and data. Moving forward, it will serve as the foundation for Derived PIV Credentials for access to DOJ data and applications from mobile devices. The expanded deployment and use of PIV Interoperable (PIV-I) cards by our state/local/tribal and industry partners will provide a powerful tool for authenticating external personnel before providing access to sensitive data. Overall, upgrading from username and password accessibility will significantly improve the security posture of the DOJ networks and applications, while simultaneously allowing for greater information sharing between DOJ components, other Federal Government agencies, and our partners outside of the Federal Government.

Information Security and Continuous Monitoring

The 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 efficiently 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

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. FY 2019 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. Investments in this area 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.

Continuous Diagnostics and Mitigation (CDM) Program

The Continuous Diagnostics and Mitigation (CDM) Program, centrally managed by the Department of Homeland Security, and implemented at DOJ, is intended to create a common baseline of cybersecurity capability and protection across the Federal Government. The program provides federal departments and agencies with CDM-certified capabilities and tools that identify and prioritize cybersecurity risks on an ongoing basis and enable cybersecurity personnel to mitigate the most significant problems first. The CDM tools also allows DOJ to better manage IT assets, helping to reduce the Department's overall attack surface.

b. IT Transformation

IT Transformation 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. This undertaking 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. Although work on these initiatives began in FY 2012, and consists of e-mail consolidation, data center consolidation, enterprise IT cybersecurity investments, and desktops, efforts are ongoing and reflected in the FY 2019 budget request.

The Department is committed to achieving "smaller and smarter" data center infrastructure with improved operational efficiency and overall cost savings. The enterprise vision for DOJ's future computing environment is to deliver standard and agile computing capabilities to authorized users as part of a services-based model. Commodity computing, storage and networking services will be provided through a combination of DOJ's internal Core Enterprise Facilities (CEFs) and external providers offering commercial cloud computing and other managed IT services. Through the DOJ Data Center Optimization Initiative (DCOI), DOJ is charting its path to achieve this enterprise vision that includes comprehensive data center inventories, multi-year strategies to consolidate and optimize data centers, performance metrics, and a timeline for agency activities and yearly calculations of investment and cost savings.

The need for data center consolidation and optimization across the Federal government continues to be as strong today as it was when first envisioned in 2010 when the Office of Management and Budget (OMB) launched the Federal Data Center Consolidation Initiative (FDCCI) to specifically:

- Promote the use of green information technology (IT) by reducing the overall energy and real estate footprint of government data centers;
- Reduce the cost of data center hardware, software, and operations;
- Increase the overall IT security posture of the Federal Government; and
- Shift IT investments to more efficient computing platforms and technologies

DOJ has made significant progress in consolidating data centers since 2010. As of July 2017, DOJ has reduced its unclassified data centers in operation from 110 to just 32, including the three CEFs. Achieving the goals and objectives of the DCOI requires more than just closing these data centers and relocating infrastructure. It requires a balanced strategy to transform the workforce, processes, and technologies used in the three interdependent elements of consolidation, shared services, and optimization.

c. Law Enforcement Information Sharing Program The Law Enforcement Information Sharing Program has been moved from JIST to the Working Capital Fund (WCF) and is now in O&M status.

d. Policy, Planning and Oversight

Office of the CIO - DOJ IT Management: JIST resources fund 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 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**

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

- The Department CIO's participation in budget planning, review, and approval. IT resource planning, reporting, and review instructions are included in the CFO's overall budget guidance, which is published each year and is 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 the CIO's 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. CIO participation in budget planning, review, and approval for major IT programs is defined in agency budget planning guidance, policy, and process descriptions. To ensure effective compliance, the OCIO worked collaboratively with the Office of Management and Budget to secure approval of this as part of the overall 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, and other statutory requirements. In addition, PPS performs reviews examining 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; a technical reference architecture. 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 on 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, 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 and with industry in the exploration of new technologies by progressing through requirements, concepts, design, component sponsorships, and prototyping that may eventually result in enhanced operational systems that support the mission and can be used across the Department.

g. Enterprise Wireless Communications

The OCIO maintains oversight and strategic planning responsibility for DOJ's use of wireless communications spectrum. This spectrum is used 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 and contractors are responsible for performing the following functions for the Department's radio/wireless/mobility programs:

- **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 innovation.
 - **Spectrum Management:** Staff serve 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.
1. 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 in emergency situations; reviewing and updating the approximately 22,000 DOJ-wide frequency assignments; and reviewing plans for spectrum relocation as a result of spectrum auctions.
 2. The staff provides guidance and oversight for the procurement of spectrum-dependent systems by obtaining spectrum certifications from NTIA. This process ensures 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 Team within the DOJ OCIO, 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 strategic objectives are met through the administration of the Wireless Communications Board (WCB).
- **Mobility Engineering:** Staff provides secure mobile communications solutions for JMD, as well as component customers. These solutions leverage Department level buying power to meet requirements at the lowest possible cost, while continuing to keep pace with the rapidly evolving mobile device hardware and software marketplace.

V. Program Increases by Item

Item Name:	Continuous Diagnostics and Mitigation (CDM)
Strategic Goal:	Performance material will be provided at a later date.
Budget Decision Unit(s):	JIST
Organizational Program:	JMD/OCIO/Cybersecurity Services Staff (CSS)

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars \$772,000

Description of Item

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.

Justification

The CDM program also provides support for training and governance activities, ensuring that CDM deployments and governance activities reinforce agency responsibilities for Information Security Continuous Monitoring as identified in OMB 14-03 as well as in the Federal Information Security Modernization Act of 2014.

Impact on Performance

The CDM program strategy results in an enterprise approach to continuous diagnostics, including consistent application of best practices that enhances government network security through automated control testing and progress tracking. This approach provides services to implement sensors and dashboards, delivers near-real time results, and prioritizes the worst problems within minutes, versus quarterly or annually. CDM also enables defenders to identify and mitigate flaws at network speed, and lowers operational risk and exploitation of government IT systems and networks.

Additionally, for federal cyber investments, the CDM program fulfills Federal Information Security Management Act (FISMA) mandates.

The CDM program is designed to rigorously ensure personal privacy. Data sent from CDM participant networks to DHS does not include any Personally Identifying Information (PII) or information about specific department or agency computers, applications or user accounts.

Funding

FY 2017 Enacted				FY 2018 President's Budget				FY 2019 Current Services			
Pos	agt/atty	FTE	\$(000)	Pos	agt/atty	FTE	\$(000)	Pos	agt/atty	FTE	\$(000)
0	0	0	\$0	0	0	0	\$0	0	0	0	\$772

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2019 Request (\$000)	FY 2020 Net Annualization (change from 2019) (\$000)	FY 2021 Net Annualization (change from 2020) (\$000)
		0	\$0	\$0	\$0
Total Personnel		0	\$0	\$0	\$0

Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2019 Request (\$000)	FY 2020 Net Annualization (change from 2019) (\$000)	FY 2021 Net Annualization (change from 2020) (\$000)
Total Non-Personnel (Hardware, Software, Contractor Support)			\$772	\$0	\$0

Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total FY 2019 (\$000)	FY 2020 Net Annualization (change from 2019) (\$000)	FY 2021 Net Annualization (change from 2020) (\$000)
Current Services	0	0	0	\$0	\$0	\$0	\$0	\$0
Increases	0	0	0	\$0	\$772	\$772	\$0	\$0
Grand Total	0	0	0	\$0	\$772	\$772	\$0	\$0

Affected Crosscuts

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