U.S. Department of Justice

FY 2020 PERFORMANCE BUDGET
Congressional Justification
Justice Information Sharing Technology

Table of Contents

I. Overview

The FY 2020 Justice Information Sharing Technology (JIST) request totals $33,875,000 and includes 33 FTE. JIST funds the Department of Justice's (DOJ) enterprise investments in information technology (IT) for technology modernization and for critical cybersecurity requirements. This submission continues supporting the IT Transformation at DOJ by moving the Office of the Chief Information Officer (OCIO) toward a service-broker management model whereby DOJ leverages industry strategic partners who expertly deliver services DOJ-wide.

As a centralized fund under the control of the DOJ Chief Information Officer (CIO), the JIST account ensures investments and shared services are well planned, coordinated amongst DOJ components, and in alignment 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 2020, the JIST appropriation will fund the DOJ CIO's continuing efforts to transform IT enterprise infrastructure and cybersecurity. These efforts include resources for OCIO's responsibilities under the Clinger-Cohen Act of 1996 and the Federal Information Technology Acquisition Reform Act (FITARA; P.L. 113-291). JIST will fund investments in cybersecurity and applications that support the overall mission of the Department and contribute to the achievement of the Attorney General's strategic goals. Electronic copies of the Department's Capital Asset Plan and Business Case exhibits can be viewed or downloaded on the IT Dashboard.

DOJ will continue its savings reinvestment strategy, enacted in the FY 2014 budget, which will support Department-wide IT initiatives. As a result, the FY 2020 Budget requests a transfer of up to $35,400,000 from DOJ components. DOJ requests that these funds remain available until expended to augment JIST resources to advance initiatives that spur IT modernization as well as invest in cybersecurity and enterprise shared services across the Department.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Cybersecurity	**Justice Security Operation Center (JSOC)**	**0**	**0**	**$2,000**	**19**
Total		**0**	**0**	**$2,000**	

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, $33,875,000 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

No substantive changes proposed.

Analysis of Appropriations Language

No substantive changes proposed.

IV. Program Activity Justification

A. Justice Information Sharing Technology – (JIST)

JIST	Direct Pos.	Estimate FTE	Amount ($000)
2018 Enacted	34	29	35,000
2019 Continuing Resolution	34	34	35,000
Adjustments to Base and Technical Adjustments	-1	-1	-3,125
2020 Current Services	33	33	31,875
2020 Program Increase	0	0	2,000
2020 Request	33	33	33,875
Total Change 2019-2020	0	0	-1,125

1. Program Description

JIST-funded programs support progress toward the Department's strategic goals by funding OCIO, which is responsible for the management and oversight of the Department's IT portfolio. The JIST appropriation funds the cybersecurity, IT modernization, Digital Services, and shared services programs, all of which support the and are relied upon by Department's agents, attorneys, analysts, and administrative staffs.

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 secure 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 priority.

The Department'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 a mature organization like CSS cannot 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; however, 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 (JSOC)

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 capabilities to protect and combat 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 or unsupportable 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 continues 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 (ISCM)

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 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)

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. The FY 2020 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 which aims to transform the Department's IT environment by driving toward a shared and less complex IT infrastructure and shifting away from government owned solutions by leveraging expert industry services offered at a more competitive price point. This undertaking directly aligns with our Data Center Consolidation/Optimization efforts, as well as with our objectives to consolidate line-of-business IT amongst smaller DOJ Offices and Divisions.

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 remains consistent: to deliver standard and agile computing capabilities to authorized users as part of a services-based model. Commodity computing, storage and networking services are now being provided through a combination of DOJ's internal Core Enterprise Facilities (CEFs) and external providers offering commercial cloud computing and other managed IT services.

DOJ has made significant progress in consolidating data centers since 2010. Notably, earlier in FY 2018 the Rockville Data Center was shuttered, which had been the Department's prime data center since 1980 and follows the closure of the Dallas Data Center in December 2015. 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. Policy, Planning and Oversight

Office of the CIO - DOJ IT Management

JIST resources fund the Department-wide IT governance, portfolio management, and oversight responsibilities of OCIO's Policy & Planning Staff (PPS). This work supports the CIO's responsibilities complying FITARA, the Clinger-Cohen Act, and other applicable laws, regulations and Executive Orders covering federal information technology management.

The OCIO provides services charged to customers with associated service expenses reimbursed via quarterly customer billings and processed through the Department's Working Capital Fund (WCF). As such, OCIO is responsible for developing service-by-service operating plans and establishing rate structures with Service Owners, preparing and validating customer billings, and conducting the day-to-day budgeting and financial management responsibilities for OCIO.

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, achieve process improvements, and ensure information security.

The Department CIO reviews and approves 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 processes.

PPS is responsible for DOJ-wide IT portfolio investment management, budget planning processes, and maintains the Department's general IT program policy and guidance documents. The investment management team organizes both the IT Acquisition Review Board and the Department's IT Investment Review Council (DIRC); both bodies help ensure alignment of component acquisitions or investments with the Department's IT strategic policies and enterprise road map. PPS also manages the work of the DOJ CIO Council, and the Department Investment Review Board (DIRB), which is led by the Deputy Attorney General. 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.

d. Enterprise IT Architecture

The Department's Enterprise Architecture (EA) programs leverages component-level programs and IT Investment Management (ITIM) principles to create a true EA framework for the federated DOJ organization. EA provides high-level guidance on IT architectural objectives as well as a central aggregation point for reporting on activities from across components to help ensure compliance with EA requirements from OMB and the Government Accountability Office. At the Department level, the EA program provides support to a wide-range of IT planning, governance, and oversight processes such as ITIM and Capital Planning and Investment Control (CPIC) as well as the DIRC and DIRB, which allows OCIO to ensure alignment of investments across the enterprise. The EA Repository contains information on all departmental system, aligns investments to these systems, and maintains the Department's IT Asset Inventory in compliance with OMB Circular A-130.

The role of the EA program continues to enhance OCIO's ability to assess opportunities for IT consolidation and utilize shared services. Within the IT Acquisition Review Board the DIRC, EA assessments drive towards system alignment objectives as outlined in the Technical Reference Architecture, such as prioritizing Cloud-first investments and code-sharing/reuse to achieve cost saving efficiencies.

e. Chief Technology Officer

The DOJ Chief Technology Officer (CTO) identifies, evaluates, and facilitates the adoption of innovative new technologies that can result in in additional value for the Department. A key objective of the CTO is to create partnerships, both across DOJ components as well as with industry, for the exploration of new technologies. By working with partners through the process the requirements gathering process to the prototyping phase, the CTO can promote the adoption of enhanced and potentially scalable solutions to support the Department's missions.

f. Wireless Communications Platforms

The OCIO maintains oversight and strategic planning responsibility for DOJ's use of wireless communications spectrum. This spectrum is used for tactical 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 and wireless 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 DOJ representative to the NTIA and other federal agencies to coordinate all national and international radio frequency (RF) spectrum access (in support of critical law enforcement [LE] functions) 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; analyzing, selecting and assigning specific/appropriate frequencies for the domestic and foreign operational deployment of RF equipment during peacetime and in emergency situations; reviewing and updating approximately 20,000 DOJ-wide frequency assignments (e.g., legal RF licenses for federal users); and reviewing plans for spectrum relocation as a result of spectrum auctions. 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.

- **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) which oversees land mobile radio, spectrum relocation, and other areas.

- **Spectrum Relocation:** Staff works with leadership, DOJ Budget Staff, and interagency partners (OMB, NTIA) to effectively transition law enforcement wireless capabilities from auctioned RF 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 (e.g., Spectrum Relocation Funds [SRF]) used to vacate spectrum and rebuild affected wireless capabilities.

2. Performance Tables

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)											
DOJ Strategic Goal/Objective: 1.2 Combat cyber-based threats and attacks & 4.4 Achieve management excellence											
RESOURCES		Target		Actual		Projected		Changes		Requested (Total)	
		FY 2018		FY 2018		FY 2019		Current Services Adjustments and FY 2020 Program Change		FY 2020 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
		34	35,000 [25,367]	29	35,000 [24,593]	34	35,000 [12,000]	-1	-1,125 [-8,334]	33	33,875 [3,666]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2018		FY 2018		FY 2019		Current Services Adjustments and FY 2020 Program Change		FY 2020	
Program Activity		FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
		34	35,000 [25,367]	29	35,000 [24,593]	34	35,000 [12,000]	-1	-1,125 [-8,334]	33	33,875 [3,666]
Performance Measure	Percentage of offenders booked through JABS	100%		100%		100%		N/A		100%	
Performance Measure	Maintain mainframe enterprise system availability for client organizations	99%		99%		99%		N/A		99%	
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations	99%		99%		99%		N/A		99%	
Performance Measure	Ensure IT systems are certified and accredited	100%		100%		100%		N/A		100%	
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms	85%		90%		85%		N/A		85%	
Performance Measure	Number of DOJ systems moved to the cloud	14		130		18		N/A		18	

	PERFORMANCE MEASURE TABLE
	Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)
	DOJ Strategic Goal/Objective: 1.2 Combat cyber-based threats and attacks & 4.4 Achieve Management Excellence

Performance Report and Performance Plan Targets		FY 2014	FY 2015	FY 2016	FY 2017	FY 2018		FY 2019	FY 2020
		Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Percentage of offenders booked through JABS	100%	100%	100%	100%	100%	100%	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	100%	100%	100%	99%	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	85%	85%	85%	90%	85%	94%	85%	85%
Performance Measure	Number of DOJ systems moved to the cloud	N/A	N/A	N/A	11	14	130	18	18

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

JIST-funded programs support the Strategic Plan for Information Services and Technology (FY 2018 – 2020) 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. The FY 2018 – 2020 Department of Justice Strategic Goals are:

- Strategic Goal 1: Enhance National Security and Counter the Threat of Terrorism.
- Strategic Goal 2: Secure the Borders and Enhance Immigration Enforcement and Adjudication.
- Strategic Goal 3: Reduce Violent Crime and Promote Public Safety.
- Strategic Goal 4: Promote Integrity, Good Government, and the Rule of Law.

Specifically, JIST supports Strategic Objective 1.2: Combat cyber-based threats, attacks; and Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

The JIST account provides resources so that OCIO can ensure investments in IT infrastructure, cybersecurity, enterprise solutions for commodity applications, and information sharing technologies are well planned and aligned with the Department's overall IT strategy and enterprise architecture. The CIO's focus remains advancing these initiatives transforming business processes, as well as prioritizing investments in enterprise mission and cybersecurity requirements.

The DIRB periodically reviews major IT investments. The Deputy Attorney General chairs the Board, and the DOJ CIO serves as vice chair. The DIRB includes the Assistant Attorney General for Administration, the Department's Controller, and various IT executives representing key DOJ components.

The DIRB provides the highest level of investment oversight as part of the Department's overall IT investment management process. The Department's IT investments are vetted annually through the budget submission process, in conjunction with each component's Information Technology Investment Management (ITIM) process. The DIRB's principal functions in fulfilling its decision-making responsibilities are to:

- Ensure compliance with the Clinger-Cohen Act, FITARA, and all other applicable laws, rules, and regulations regarding IT and information resource 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 system 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 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.

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 support the DOJ IT Intake process through which commodity IT acquisitions are reviewed against architectural, procurement, and vendor management standards. The Department contributes to the Federal IT Dashboard that allows management review over 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.

b. Strategies to Accomplish Outcomes

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

Cybersecurity

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

- **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.

- **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 leverage Continuous Diagnostics and Mitigation (CDM) offerings and will deploy a privileged account manager system and mature the identity and access management system, resulting in a more secure enterprise by increasing the level of assurance for privileged users as well as the ability to provide insight and access control to identities who access DOJ data and resources. As physical boundaries to network access dissolve, the identity is becoming the new perimeter and it is imperative to ensure that the right people are accessing DOJ resources.

- **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.

- **DOJ's Insider Threat Prevention and Detection Program (ITPDP):** 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.

- **Continuous Diagnostics and Mitigation (CDM):** The CDM program enables government entities to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. CDM offers commercial off-the-shelf (COTS) tools, with robust terms for technical modernization as threats change. Summary information can feed into an enterprise-level dashboard to inform and situational awareness into cybersecurity risk posture across the federal government.

IT Transformation

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

- **Enterprise E-mail Consolidation:** The Department's email consolidation is a long-term, multi-year effort. In Phase 1 (FY 2012 – FY 2015), DOJ consolidated 23 disparate email systems to nine systems. In addition, new and enhanced enterprise messaging and collaboration services were introduced to components. In Phase 2 (FY 2016 – FY 2020) under a Cloud Service Provider (CSP) model, DOJ is

enhancing IT resiliency and office productivity by moving its approximately 170,000 users to a common Office 365 desktop baseline while continuing to merge and reduce the number of communication systems. The Department has migrated nearly 110,066 mailboxes as of February 2019.

- **Data Center Consolidation:** Since 2010, the Department has worked towards reducing its data center footprint (110 unclassified data centers of varied size) and optimizing its IT infrastructure, as part of the enterprise vision to deliver standard and agile computing that maximizes mission capabilities. DOJ has made considerable progress toward these goals. In FY 2014, DOJ designated three data centers as Core Enterprise Facilities (CEFs) to support DOJ's future enterprise requirements for data centers. These three CEFs enable DOJ 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. One of the keys to reducing the footprint to these three CEFs is migrating a significant portion of the infrastructure to cloud computing. Cloud platforms provide scalability, flexibility, accessibility, availability, enhanced security and economies of scale, provides faster implementation, streamlined procurement, and improved performance. As of February 2019, the Department has closed 89 data centers since 2010, including the Rockville Data Center in 2018, and the Dallas Data Center in 2015. DOJ expects to close 12 additional data centers by the end of FY 2019 and the remaining 6 unclassified centers by the end of FY 2020. With an optimization strategy that is multi-threaded, DOJ is driving cost efficiencies, data interoperability and an improved customer experience; with virtualization, cloud computing and managed services at the core. The DOJ is on pace to achieving its enterprise vision through multi-year strategies to consolidate and optimize data centers and its entire IT infrastructure.

- **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 to expand the set of available device options in order to better fit the need of the user. Several components are planning Justice Consolidated Office Network (JCON) workstation refreshes so the Enterprise Desktop team will continue to work closely with components to reuse these common solutions and standards across groups.

Digital Transformation

Digital Transformation is responsible for driving the efficiency and effectiveness of the agency's highest-impact digital services. The Department will continue to coordinate with digital services' organization such as the U.S. Digital Service and the General Services Administration's Technology Transformation Service (e.g. 18F) to institutionalize digital competencies and apply it to government work by setting standards, introducing a culture of technological accountability, and assessing common technology patterns that can be replicated across agencies.

The Department continues to embrace examples and concepts from these organizations as it evaluates programs through its governance role assessing what, if any, IT initiatives or programs may be served best by introducing a Digital Service Team. The current IT environment across the Department is focusing principally on securing deployed assets buffering them from cyber-attacks, and addressing high-risk legacy systems and networks, leaving little funding for true IT initiative development and modernization on which Digital Service teams might take an active participatory role.

The Department previously coordinated with USDS on leveraging the associated Schedule A hiring authority in order to bring private sector expertise that will help progress the IT transformation effort already underway within OCIO. These Information Technology Distinguished Fellows (IT Fellows) are recruited to leverage their specific skill sets needed to truly transform the OCIO to a service broker model. These are term positions that will come in and address critical risks and issues, much as in the same way as proffered under USDS, but on IT initiatives not necessarily requiring rescue. The Department will continue to identify any IT programs that would benefit from specific attention offered by a USDS-style approach and coordinate closely with external digital service organizations on any future engagement as appropriate.

Cyberspace

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, along with the FBI and collaborating agencies will continue to work with industry in order to learn and share strategies with a goal of providing new insights into our critical mission needs.
By supporting the National Strategic Computing Initiative, the Department will continue 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/Data Analytics

The OCIO plays a leading role in the Department's approach to the big data challenge, and initiated a strategic plan for information management, access and sharing that provides structure, guidance, and oversight for the identification, control, and leveraging of our data resources to realize their maximum value and appropriate use. A data management program was initiated to implement this strategy and collaborate fully with the various mission support areas of records management, law enforcement and litigation. The OCIO continues to address the challenge area of ensuring appropriate access to mission data for high-speed data ingest and analytics and associated resources within a shared environment where appropriate to process big data. This includes enabling efficient access to such analytics tools while also decreasing redundancy and increasing economies of scale through such methods like blank purchase or enterprise license agreements. Additionally, DOJ remains engaged with private industry to identify and evaluate new technologies and analyze the ever-increasing volume of investigative, discovery and litigation data. Taken together, these efforts place the Department on a path to mature our data capabilities which will in the end provide better support to our various missions.

V. Program Increases by Item

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

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

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $ 2,000,000

Description of Item

The JSOC provides 24x7 monitoring of the Department's internet gateways and responds to cyber threats to DOJ through real-time detection of threat activity, analytics, incident management and response. It analyzes threat intelligence, identifying indicators of compromise, which it uses to configure the DOJ enterprise sensor grid. The JSOC leads and coordinates the Department's cybersecurity response actions with external Federal Agencies and law enforcement. It also supports secure engineering by reviewing all requests for external network connectivity, integrating log files into security analytics systems and managing intrusion detection system configuration. All of which provides the JSOC with the ability to detect and mitigate advanced adversary intrusions with minimal disruption to mission services.

Justification

Threat capabilities continue to evolve. DOJ is seeing more complex attacks that do not leave file based indicators and are not detected by traditional signature based network detection systems. Malicious files stay resident in memory and leverage compromised credentials to avoid detection. Additionally, the expansion of cloud and mobile technologies introduce new attack vectors into DOJ's network architecture.

The $2.0 million JIST enhancement request will allow DOJ to improve security monitoring at all levels, following DOJ data from core data centers to cloud environments. To protect high value assets and information in DOJ data centers JSOC must extend its sensors deeper into DOJ's network architecture, integrating behavior-based sensors at strategic network locations. As cloud and mobile technologies dissolve DOJ's network perimeter, JSOC must also extend its detection and response capabilities beyond the on-premises network to wherever our data resides.

The Department of Justice is especially attractive to cyber attackers because of its law enforcement, litigation, incarceration, civil protection, and national security missions. Extending DOJ's detection and response capabilities into cloud service providers, and core enterprise facilities increases JSOC's ability to detect and respond to modern threat capabilities earlier in the attack lifecycle and limit damage.

Impact on Performance

The JSOC provides enterprise cybersecurity for the Department, ensuring the confidentiality, integrity and availability of the Department's information and information systems. Investments in detection and response capabilities advance the JSOC's ability to prevent, contain and

eliminate threat activity before it has a chance to establish a persistent presence in DOJ networks, thereby, limiting data loss, impact to systems, and preserving DOJ's law enforcement mission.

Behavioral based network sensors in core data centers protect DOJ High Value Assets and Mission Essential Systems. They provide defense in depth to the internet gateway sensors and a complimentary ability to detect advanced threat activity that would otherwise go unnoticed by signature-based sensors.

Cloud based detection and response systems extend JSOC's reach to cloud environments and advance its ability to monitor an increasingly complex environment, where a single misconfiguration can expose vast amounts of DOJ information. With these investments, the JSOC will monitor the secure configuration of DOJ's cloud environment, thus minimizing the attack surface and preventing intrusions. If an intrusion should occur, JSOC will detect the activity early in its attack lifecycle, isolate and defeat the threat.

Funding

FY 2018 Enacted				FY 2019 Continuing Resolution				FY 2020 Current Services			
Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)	Pos	agt/ atty	FTE	$(000)
0	0	0	$0	0	0	0	$1,439	0	0	0	$1,439

Personnel Increase Cost Summary

Type of Position/Series	Modular Cost per Position ($000)	Number of Positions Requested	FY 2020 Request ($000)	FY 2021 Net Annualization (change from 2019) ($000)	FY 2022 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 2020 Request ($000)	FY 2021 Net Annualization (change from 2020) ($000)	FY 2022 Net Annualization (change from 2021) ($000)
Total Non-Personnel (Hardware, Software, Contractor Support)			$2,000	$-2,000	$0

Total Request for this Item

	Pos	Agt/ Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total FY 2020 ($000)	FY 2021 Net Annualization (change from 2021) ($000)	FY 2022 Net Annualization (change from 2022) ($000)
Current Services	0	0	0	$0	$1,439	$1,439	$0	$0
Increases	0	0	0	$0	$2,000	$2,000	$-2,000	$0
Grand Total	0	0	0	$0	$3,439	$3,439	$-2,000	$0

Affected Crosscuts

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