U.S. DEPARTMENT OF JUSTICE

Justice Information Sharing Technology

FY 2025 PERFORMANCE BUDGET
Congressional Justification

Attachment A

Table of Contents

I. Overview for Justice Information Sharing Technology

The Fiscal Year (FY) 2025 Justice Information Sharing Technology (JIST) request totals $202.4 million and includes 59 authorized positions and 47 full-time equivalents (FTE). This budget represents an increase of $64.4 million from the FY 2023 Enacted Budget and includes funds for current services adjustments and three program enhancements.

JIST funding supports the Department of Justice (the DOJ, Department) enterprise investments in Information Technology modernization and critical cybersecurity requirements. As a centralized fund under the control of the DOJ Chief Information Officer (CIO), the JIST account ensures investments and shared services are in alignment with the DOJ's overall IT strategy, cybersecurity strategy, and enterprise architecture. CIO oversight of the DOJ IT environment is critical given the level of dependence on the IT infrastructure and cybersecurity posture necessary to conduct legal, investigative, and administrative functions throughout the Department. This submission continues moving the Office of the Chief Information Officer (OCIO) toward leveraging industry strategic leaders and partners to deliver advanced services DOJ-wide.

In FY 2025, the JIST appropriation will fund OCIO's continuing efforts to provide innovative technologies and services in support of the President's Management Agenda and the Attorney General's Strategic Plan for FY 2022-2026. Program areas include cybersecurity, IT transformation, IT architecture and oversight, and innovation engineering.

The DOJ will also support enterprise IT initiatives by continuing the strategy of reinvesting cost savings. Through this strategy, the Department's FY 2025 budget requests the authority to transfer up to $40.0 million from the DOJ components and that these funds remain available to the OCIO until expended. These funds provide DOJ with the flexibility to IT modernization initiatives in enterprise cybersecurity and other services for the benefit of the entire Department.

II. Summary of Program Changes

Item Name	Description	Positions	FTE	Amount ($000)	Page
Cybersecurity Posture Enhancements	Continue transition from traditional network access monitoring to identity-based access for applications and data; enhancements to cloud environment to improve security response; implementation of event logging across Department devices to enable visibility before, during, and after incidents	6	3	$51,540	15
EO 14110 Implementation (Artificial Intelligence)	Create Department-level AI governance and enablement capability to provide thoughtful risk management, support workforce development, and drive innovation and adoption of AI.	1	1	$2,460	21
National Law Enforcement Accountability Database	Establishing a National Law Enforcement Accountability Database in accordance with Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety."	2	1	$10,000	25

III. Appropriations Language and Analysis of Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, [$193,630,000] *$202,395,000* to remain available until expended: Provided, That the Attorney General may transfer up to $40,000,000 to this account, from funds made available to the Department of Justice 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: Provided further, That any transfer pursuant to the first proviso shall be treated as a reprogramming under section 504 of this Act and shall not be available for obligation or expenditure except in compliance with the procedures set forth in that section.

Analysis of Appropriations Language

No substantive changes proposed.

IV. Program Activity Justification

A. *Justice Information Sharing Technology*

Justice Information Sharing Technology	Direct Pos.	Estimate FTE	Amount (000s)
2023 Enacted	50	31	$138,000
2024 Annual Continuing Resolution*	50	42	$138,000
Adjustments to Base and Technical Adjustments	0	0	$395
2025 Current Services	50	42	$138,395
2025 Program Increases	9	5	$64,000
2025 Request	59	47	$202,395
Total Change 2024-2025	**9**	**5**	**$64,395**

***** All references in this document and tables to an FY 2024 Continuing Resolution are to an FY 2024 Annualized Continuing Resolution.

1. Program Description

The DOJ CIO is responsible for the management and oversight of programs supporting the DOJ's enterprise IT portfolio. Using JIST funds, OCIO enables innovative technologies and services to support the DOJ's overall strategic goals and objectives. JIST also allows the OCIO to provide oversight and execution of the DOJ IT projects in alignment with Department architectures and sound management principles. The FY 2025 JIST funding request supports advances in cybersecurity, IT transformation, IT architecture and oversight, and innovation engineering; all of which support and are relied upon by DOJ agents, attorneys, analysts, and administrative staffs.

a. Cybersecurity

Enhancing the DOJ's cybersecurity posture remains a top priority for the Department and its leadership, as the DOJ supports a wide range of missions including national security, law enforcement, and impartial administration of justice. The systems supporting these critical missions must secure sensitive information, enable essential workflows, and protect the integrity of data and information guiding vital decision-making.

DOJ's OCIO provides enterprise-level strategy management, policy development, as well as tools and monitoring capabilities to support Department-wide security operations. While the OCIO continues to improve these services, the costs for personnel, hardware, and software continue to rise. At the same time, workloads for existing responsibilities have increased, and threats to our systems have skyrocketed. As such, the OCIO will continue investing in the following programs to support the DOJ components in protecting mission assets from today's dynamic threat environment.

(1) Enhanced Cybersecurity Architecture

With the increasing sophistication of adversarial threats, it is essential for the DOJ to expand its risk management capabilities by employing strategic enterprise-wide cybersecurity investments to enhance the Department's security posture. Increasing the security of the DOJ is a significant undertaking that requires substantial investments in the requirements, architecture, design, and development of systems,

system components, applications, and networks. The Department will continue to refine its risk management capabilities and processes by observing lessons learned in the evolution of the threat landscape.

The DOJ plans to integrate information and insights gained from the SolarWinds incident into its broader IT modernization efforts, budget discussions, mission delivery activities, and security initiatives to reduce duplication and ensure alignment and prioritization of remediation activities across the Department. The OCIO continues to modernize endpoint detection and response, event logging, cloud security, authentication, encryption, and security operations to improve detection and response attacks, as well as to limit their impact.

The DOJ will continue its transition to a zero-trust architecture (ZTA), a system environment designed to reduce the uncertainty in enforcing accurate, per-request access decisions for information systems and services. By moving away from traditional network access monitoring to identity-based access for applications and data, ZTA enables the DOJ resources to access applications and data while providing protection from targeted phishing attacks. As part of its ZTA transition, the DOJ plans to implement enhanced endpoint detection and response, phishing-resistant Multi-Factor Authentication (MFA), centralize authentication, and capture log details from the new architecture.

(2) Justice Security Operations Center (JSOC)

The OCIO maintains and operates the JSOC, providing around-the-clock monitoring and incident response management of the DOJ internet gateways. The JSOC continues to identify increases in email, cloud, and mobile device attacks. Adversaries have become increasingly automated and complex, requiring the DOJ to continuously develop and deploy modern defensive capabilities to counter these efforts. Paradigm shifts in IT, such as cloud computing and ubiquitous mobility, also place an increased emphasis and workload on cybersecurity. As the DOJ embraces new technologies, the OCIO must ensure secure deployment to safeguard data while supporting the DOJ operational missions.

The DOJ continues to invest in infrastructure modernization across the DOJ's geographically dispersed footprint and adapt to the changing technological landscape associated with cloud and mobility, or else faces an environment of degraded effectiveness by aged or unsupported infrastructure.

(3) Identity, Credential, and Access Management (ICAM)

The ICAM program establishes a trusted identity for every DOJ user and provide controls to ensure the right user is accessing the right resources at the right time. The program reduces reliance on password-based authentication, centralizes privileged user management, and automates enforcement of identity and access policies. Replacing username and password accessibility with Personal Identity Verification (PIV)-based authentication will significantly improve the security posture of the DOJ networks and applications, while simultaneously allowing for greater information sharing between the DOJ components, Federal Government agencies, and partners outside of the government.

(4) Information Security and Continuous Monitoring (ISCM)

The ISCM program brings together enterprise-wide security tools and technologies to support continuous diagnostics, mitigation, and reporting, as well as Federal Information Security Modernization Act (FISMA) system security authorization requirements across the DOJ components. ISCM's suite of tools and services include:

- Automated asset, configuration, and vulnerability management;
- Networks and systems scanning 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.

The program continuously expands on the suite of analytics to provide the DOJ analysts and leadership with consistent and reliable tools to support the security of mission-enabling systems. The OCIO is also improving the security posture of the DOJ's High Value Assets through new processes and tools to help identify, assess, and remediate vulnerabilities at the enterprise level.

(5) Insider Threat Prevention and Detection Program (ITPDP)

The ITPDP is responsible for protecting sensitive (e.g., controlled unclassified information, law enforcement sensitive) and classified information and resources from misuse, theft, unauthorized disclosure, or espionage by insiders. The DOJ ITPDP, established under Executive Order 13587, directed executive branch departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs. The ITPDP works with the DOJ's Security and Emergency Planning Staff's (SEPS) efforts to implement Insider Threat and Security, Suitability, and Credentialing Reform (ITSCR) throughout the Department.

The DOJ requires the capacity to detect patterns and correlated indicators across multiple types of information (e.g., human resources, information assurance, security, and counterintelligence) to prevent or mitigate threats and adverse risks to the security of the United States. The OCIO continues to expand monitoring capabilities to reduce risk from insider threats, including expansion of infrastructure to cover new systems and personnel, as well as adoption of analytics to develop alters and triggers for common insider threat behaviors.

(6) Continuous Diagnostics and Mitigation (CDM)

The CDM program, centrally managed by the Department of Homeland Security and implemented at the DOJ, creates a common baseline of cybersecurity capabilities across the Federal Government. The program provides departments and agencies with CDM-certified technologies and tools to identify and prioritize cybersecurity risks on an ongoing basis, allowing cybersecurity personnel to prioritize the most significant problems first. CDM tools allow the DOJ to manage IT assets efficiently and help reduce the Department's overall attack surface.

b. IT Transformation

IT transformation is an ongoing OCIO commitment to evolve the DOJ's IT environment by driving toward shared commodity infrastructure services and simplified design and implementation of tools to advance the mission. These efforts allow the DOJ to shift from custom government-owned solutions to advanced industry-leading offerings at competitive pricing. The OCIO recognizes modernization as an ongoing activity, requiring IT strategies to adapt as technology changes.

The Department is committed to achieving "smaller and smarter" data center infrastructure with improved operational efficiency and overall cost savings. The enterprise vision for the 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 provided through a combination of the DOJ's internal Core Enterprise Facilities (CEFs) and external providers offering commercial cloud computing and other managed IT services.

(1) Data Center Transformation and Optimization

The DOJ provides commodity computing, storage, and networking services through a combination of CEFs, commercial cloud computing providers, and other managed IT services. This aligns with the DOJ's Data Center Transformation Initiative (DCTI), the underlying consolidation strategy for data centers operated by the Department, as well as the objectives to consolidate and modernize enterprise infrastructure. The OCIO will continue to optimize CEF operations and cloud environments to achieve cost savings, simplify end-user experience, and improve customer service.

(2) Email and Collaboration Services (ECS)

The DOJ was one of the first Federal agencies to transition from multiple disparate email systems to a single, shared, cloud-based infrastructure. In addition to reducing enterprise costs and increasing security, the transition improves user experiences across the DOJ offices regardless of location or device. The first phase of ECS transitioned email to a common system, while the next phases will deploy technologies to ensure real-time data sharing and enhanced collaboration. These include fully auditable secure file sharing between components, a unified communications system to facilitate mobile and remote collaboration, as well as additional capabilities to connect the DOJ with the larger law enforcement community, including state, local, tribal partners, and external litigators.

c. IT Architecture and Oversight

The OCIO provides guidance on IT architectural objectives and serves as a central aggregation point for reporting on activities from across components to help ensure compliance with enterprise architecture (EA) requirements from OMB and the Government Accountability Office (GAO). The OCIO supports a wide range of IT planning, governance, and oversight processes, including IT investment management and Capital Planning and Investment Control (CPIC), as well as the Department Investment Review Council (DIRC), which allows OCIO to ensure alignment of investments across the enterprise. The EA repository contains information on all departmental systems, aligns investments to these

systems, and maintains the Department's IT Asset Inventory in compliance with OMB Circular A-130, Managing Information as a Strategic Resource.

Oversight of the DOJ IT environment by the CIO is vital given the role of technology in supporting the DOJ's varied legal, investigative, and administrative missions. JIST resources fund the DOJ-wide IT architecture governance and oversight responsibilities of the OCIO. These efforts support the CIO's responsibilities in complying with the Federal Information Technology Acquisition Reform Act (FITARA), the Clinger-Cohen Act, and other applicable laws, regulations, and Executive Orders governing federal IT management.

DOJ Order 0903 defines the Department's policies with respect to IT management, which account for provisions enacted in FITARA, and details the DOJ CIO's role in IT budget planning and execution, including:

- Participation in budget planning, review, and approval. IT resource planning, reporting, and review instructions are included in the Chief Financial Officer's (CFO) overall budget guidance, which is published each year and is coordinated with the formal Spring Call budget formulation process; and
- 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 OCIO also leverages the DIRC, made up of key DOJ and component executives, to monitor and support major, high-visibility IT projects and services. Additionally, the DIRC evaluates IT budget enhancement requests, among other responsibilities. The CIO Council and IT Acquisition Review (ITAR) processes also provide oversight, risk reduction, and insight into IT programs across the DOJ. These mechanisms provide opportunities to address key challenges at both the program and enterprise levels to develop solutions addressing mission and business needs.

d. Innovation Engineering

The OCIO facilitates adoption of new and innovative technologies to support the DOJ mission requirements. By creating partnerships with the DOJ components, federal agencies, and industry leaders for the exploration of new technologies, the OCIO leads the ideation, design, planning, and execution of enterprise IT innovations to enhance the DOJ user experiences while ensuring alignment with the DOJ architectures and strategic priorities. The OCIO also uses technology readiness assessments to evaluate the maturity of technologies and readiness for incorporation into a system, as less-than-ready technologies can be the source of program risks, delays, and cost increases.

By applying human-centered design principles to understand DOJ operational needs, the OCIO facilitates the innovation management lifecycle to enable best-in-class services. Examples include advanced technologies such as robotic process automation, artificial intelligence, machine learning, and advanced analytics. In addition to operationalizing a DOJ-wide data strategy to address privacy, security, interoperability, and data management, the OCIO developed a DOJ AI strategy to maximize support and published its Artificial Intelligence (AI) use case inventory on justice.gov.

2. Performance and Resources Tables

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: Justice Information Sharing Technology (JIST)												
RESOURCES ($ in thousands)			**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
			FY 2023		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2025 Program Changes**		**FY 2025 Request**	
Total Costs and FTE			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			42	138,000	31		42	138,000	5	64,395	47	202,395
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2023**		**FY 2023**		**FY 2024**		**Current Services Adjustments and FY 2025 Program Changes**		**FY 2025 Request**	
Program Activity			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			42	138,000	31		42	138,000	5	64,395	47	202,395
Performance Measure:	1.2	Percent of Department websites reflecting U.S. Web Design System requirements and meeting best practices for plain language and user centered design	20%		100%		100%		0		100%	
Performance Measure:	1.2	Percent of common data sets accessible amongst DOJ components.	10%		48%		49%		0		49%	
Performance Measure:	2.4	Percent of confirmed cyber incidents to Department systems.	<.001%		0.00%		<.001%		0		<.001%	

Strategic Objective	PERFORMANCE MEASURE TABLE						
	Decision Unit: Justice Information Sharing Technology (JIST)						
	Performance Measures		FY 2022	FY 2023	FY 2023	FY 2024	FY 2025
			Actual	Target	Actual	Target	Target
1.2	**Performance Measure**	Percent of Department websites reflecting U.S. Web Design System requirements and meeting best practices for plain language and user centered design.	100%	100%	100%	100%	100%
1.2	**Performance Measure**	Percent of common data sets accessible amongst DOJ components.	47%	48%	48%	49%	50%
2.4	**Performance Measure**	Percent of confirmed cyber incidents to Department systems.	.0004	<.001%	0.00%	<.001%	<.001%

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

In FY 2025, JIST-funded programs will support the Attorney General's priority area of cybersecurity by providing enterprise IT infrastructure and secure environments necessary to conduct national security, legal, investigative, and administrative functions. Specifically, JIST supports combating cyber-based threats and attacks and achieving management excellence through innovation to promote good government.

The OCIO's strategic initiatives and priorities are:

- Continuously improve service delivery;
- Effectively invest in technology;
- Protect critical mission assets; and
- Build innovative capabilities.

JIST resources fund the management, design, engineering, and deployment of specific business and mission critical IT infrastructure investments. It also supports the OCIO in ensuring investments in IT are well planned and aligned with the Department's overall IT strategy and enterprise architecture. The CIO remains focused on advancing these initiatives to transform business processes, as well as prioritizing investments in enterprise mission and cybersecurity.

b. Strategies to Accomplish Outcomes

(1) IT Transformation – Continuously Improve Service Delivery

As a provider of high-performing, resilient, and efficient services supporting the DOJ's missions, the OCIO must transform the delivery of current and new IT services to end users. The OCIO continues to deliver reliable services to maximize the use of cloud computing and modern applications, increase productivity through new communication and collaboration tools, and develop strategic relationships with business partners to enable self-service processes through increased intelligence in workflows and automation.

This effort is a long-term, multiyear commitment to transform the Department's IT enterprise infrastructure and centralize commodity IT services. The Department is currently undertaking the following projects:

- **Consolidated Enterprise Infrastructure:** Modernizing networking and telecommunication infrastructure to take advantage of commercially managed services and technologies to achieve greater cost efficiencies, better performance, and improved security posture.
- **Data Center Transformation:** Consolidation activities by optimizing CEF operations through new processes and tools, migrating systems to cloud environments, and performing an application rationalization activity expected to achieve cost savings, simplify end-user experience, and improve customer service.

- **Email and Collaboration Services:** Consolidating disparate systems and users into a common, cloud-hosted baseline to achieve seamless collaboration between DOJ components and external law enforcement partners.
- **Assisted/Unassisted Automation:** Strategically integrating assisted and unassisted robotic processing and chatbot automation within common and repetitive workflows to increase productivity, security, and integrity while also reducing total cost of ownership.

(2) IT Architecture and Oversight – Effectively Invest in Technology

As stewards of taxpayer funds, the DOJ will continue to seek ways to optimize the return on investments of our work and reduce the costs incurred by Department components. This will be accomplished through standardizing and simplifying technology, offering shared services and strategic sourcing, and leveraging IT governance to drive collective investment decisions.

The DOJ supports efforts to effectively invest in technology and accomplish the objectives of the DOJ's IT strategy, including the DIRC, CIO Council, and Federal IT Dashboard Report.

(3) Cybersecurity – Protect Critical Mission Assets

With threats to the DOJ increasing in frequency and complexity, protecting the DOJ mission assets continues to be a top priority for the OCIO. As such, the OCIO continues to enhance the following areas:

- **JSOC:** Proving 24x7 cyber defense capabilities critical to protect the missions of the DOJ and partner agencies through advanced modeling, detection, and analysis;
- **ICAM:** Ensuring the right people are accessing the right DOJ resources at the right time;
- **ISCM:** Hosting cyber infrastructure and providing resiliency and centralized security control management while enabling visibility into the security health of the organization;
- **ITPDP:** Discovering, deterring, and mitigating DOJ's insider threats using counterintelligence and cybersecurity monitoring tools; and
- **CDM**: Expanding DOJ's continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, and prioritizing risk alerts.

(4) Innovation Engineering – Build Innovative Capabilities

As the DOJ mission advances, the OCIO must modernize IT systems and integrate innovative technologies to support its workforce. In addition to improving current services, the DOJ must also introduce innovative capabilities and mobile-accessible solutions for more effective and timely decision-making. By applying human-centered design principles to understand the DOJ operational needs, the OCIO facilitates the innovation management lifecycle to enable best-in-class services.

V. Program Increases by Item

Item Name: **Cybersecurity Posture Enhancements**

Budget Decision Unit(s): Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions 6 Agt/Atty 0 FTE 3 Dollars $51,540,000

Description of Item

The enhancement request of $51.5 million and six positions will provide resources for implementation of cybersecurity posture enhancements in response to Executive Order 14028, Improving the Nation's Cybersecurity, OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures, OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response, OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, while addressing other opportunities to improve the Department's cybersecurity defense and resilience. The additional positions will plan execution, deployment, and operation of the technology to make sure these capabilities are developed and integrated throughout the Department. The following initiatives will be funded by this enhancement request:

- Cybersecurity Event Logging - $ 31,400,000; 4 positions
- Zero Trust Architecture for Unclassified Systems - $6,400,000; 2 positions
- Zero Trust Architecture for National Security Systems - $13,700,000; 0 positions

Justification

Cybersecurity Event Logging Enhancement – $31.4M, 4 positions

Major incidents, such as SolarWinds, underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on the DOJ information systems is invaluable in the detection, investigation, and remediation of cyber threats.

In accordance with OMB M-21-31, the DOJ is required to log data across all of the Department's approximately 200,000 devices. This represents a significant increase from the initial FY 2022 logging capacity of 7 terabytes (TB) per day, prior to the guidance provided in M-21-31. This increase will result in a new logging capacity of approximately 81 TB per day, which will add to the total amount of audit data that will need to be retained. With the FY 2023 funding, the DOJ achieved a logging capacity of 9 TB per day which was a 33% increase from FY 2022. In response to the above requirement, the DOJ will further increase its logging capacity to 34 TB

per day. This increase will extend the duration of historical log data requirements from 12 months to 30 months, thereby contributing to increased costs of storing over 28 times the amount of data. Using the additional logging, the DOJ will develop automated hunt and incident response playbooks, which will take advantage of Security, Orchestration, Automation, and Response (SOAR) capabilities. The DOJ is estimating a significant increase in the annual cost for storage, technical capabilities, as well as additional full-time personnel resources, to meet all the above requirements.

Additionally, by applying User and Entity Behavioral Analytics (UEBA), the Department will focus on preventing deliberate and intended actions, such as malicious exploitation, theft, destruction of data, and the compromise of networks, communications, or other information technology resources. UEBA capabilities allow the Department to take advantage of machine learning capabilities to detect attacks among the trillions of events ingested into the JSOC each day, a feat that would be impossible without these enhancements.

Zero Trust Architecture for Unclassified Systems – $6.4M, 2 positions

Executive Order 14028 and OMB M-22-09 require all agencies to develop a plan to implement a zero-trust architecture (ZTA). The federal government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. The Department plans to implement a ZTA, advanced endpoint detection and response, and phishing-resistant Multi-Factor Authentication (MFA). A transition to a zero-trust approach to security provides a defensible architecture for this new environment. While components have key responsibilities in ZTA, JIST will lead the department's enterprise ZTA in three key areas. Leading the creation of a unified identity provider that will secure identity across all Department systems. Improving network access, including remote access, while simultaneously improving cross-component access across Department networks, requires an enterprise approach and solution. Lastly, ensuring enterprise-wide visibility of Department endpoints through Endpoint Detection and Response (EDR) enables the JSOC to be more proactive and collaborative with all Department components. The Department will also capture device-level log details from the new architecture to improve analysis before, during, and after an attack.

- Endpoint Detection and Response

The DOJ requires an integrated set of detection and protection technologies deployed at the device level to prevent attacks, detect malicious activity, and enable holistic investigation and remediation in response to security incidents and alerts. Device protection platforms integrate machine-learning, behavioral analytics, and anomaly detection to provide a proactive approach to safeguarding endpoints, regardless of location or networks. A cloud-based option is best suited to support rapid deployment and scalability, providing comprehensive coverage for all laptops, mobile phones, desktops, and servers. The DOJ established the capability under the Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation (CDM) program. Although this program's financial support will end in FY 2025, this enhancement will maintain the capability.

- Security Operations Center Maturation

The DOJ is implementing a zero-trust architecture to allow the Justice Security Operations Center (JSOC) to monitor and defend the DOJ enterprise. ZTA enables the JSOC to shift from traditional network access monitoring towards identity-based access to applications and data. ZTA allows the DOJ employees to access applications and data they need to do their jobs while protected from targeted, sophisticated phishing attacks. DOJ devices are consistently tracked and monitored, and the security posture of those devices is considered when granting access to internal resources. DOJ systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted. These improvements will require personnel to monitor additional logs and alerts.

- Multi-Factor Authentication/Encryption

In alignment with OMB M-22-09, the Department is moving to a centralized identity provider and authentication model. This shift eliminates the individual federated component trust model, which was exploited in the SolarWinds incident, and creates a universal, mandatory multi-factor authentication. Under this model, identities and application access will be managed centrally, with Personal Identity Verification (PIV) as the standard authentication method, as mandated by OMB. However, when DOJ personnel cannot use PIV, alternate strong, phishing-resistant MFA methods are required. To achieve this, the Department will use a combination of industry standards, including FIDO2 tokens and Web Authentication.

Zero Trust Architecture for National Security Systems – $13.7 million, 0 positions

Per NSM-8, the Department must secure sensitive information stored within the National Security Systems (NSS) infrastructure. Without a comprehensive ZTA for NSS, the Department risks its most sensitive classified data and mission-essential activities, especially through information-sharing networks like Secure Internet Protocol Router System and Joint Worldwide Intelligence Communication System.

This capability is critical for the OCIO to enhance the Department's ability to prevent and mitigate threats. In alignment with policy guidance of the Executive Order 14028 and NSM-8, the use of zero trust technology and services provide an opportunity to improve the Department's security posture. The Department must increase its capacity to have expert knowledge of zero trust technology and services and resources to monitor, investigate, and respond to advanced threats.

<u>Impact on Performance</u>

The evolving threat landscape has made traditional perimeter-based network defenses obsolete. Adversaries focus on identity, lateral movement, and end-user systems to try to gain access to the Nation's most critical systems. The Department's ZTA addresses both internal and external threats by shifting to an identity-centric approach that contextually analyzes every user each time they attempt to access an application. Access will no longer be driven by whether a user was granted access to the network but will instead be based on a holistic approach that focuses on the application, user, and device. The DOJ's ZTA ecosystem requires software-defined policies to permit dynamic decisions, which allows the DOJ to adjust permissions and enable increased

access to applications when needed, but also restrict and protect access when inconsistent user behavior is detected. ZTA addresses these areas via central IDP, identity-based access control through a broker, and advanced endpoint monitoring with EDR. Without evolving DOJ security and implementing a comprehensive ZTA, the Department risks relying on outdated security protocols to secure data and access, as well as the potential for incidents similar to the SolarWinds breach.

The additional resources are necessary for the Department to avoid the risk of implementing cloud services that become avenues for exploitation by adversaries. In tandem with the acceleration to secure cloud services, the Department must increase its capacity to have expert knowledge of cloud systems and services, pervasive cloud security posture assessment, and resources to monitor and investigate within the cloud. The DOJ must maintain near-real-time visibility of assets, including those in the cloud, to ensure their security.

Moreover, the current levels of event logging are not sufficient in meeting the requirements of OMB M-21-31 nor effectively provide the Department adequate visibility and transparency into our enterprise systems. Advanced adversaries require detecting small anomalies in device and user behavior. Without logging and analyzing enough normal behavior detecting an advance actor's anomalous activity is improbable. Without significant investment into resources, the Department remains vulnerable to insufficient monitoring and understanding of ongoing cyber threats and attacks, and a lack of comprehensive data enabling critical incident response decisions. The lack of logging will limit the Department's ability to scope attacks within the trillions of events ingested into the JSOC each day.

Without the requested program enhancements, the Department lacks the full capability to successfully identify and defend against advanced threats aiming to disrupt the Department's missions and compromise sensitive DOJ data.

Funding

1. Base Funding

FY 2023 Enacted				FY 2024 Annual Continuing Resolution				FY 2025 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
21	0	15	112,078	30	0	26	112,539	30	0	30	112,934

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Info Technology Mgmt (2210)	752	6	244	143	26	858	156
Total Personnel	**752**	**6**	**244**	**143**	**26**	**858**	**156**

3. Non-Personnel Increase/Reduction Cost Summary

The enhancement request includes contractual and advisory services to provide ongoing information technology development and associated software support.

Non-Personnel Item	FY 2025 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Contract Labor	27,255	N/A	N/A	545	1,390
Software	23,533	N/A	N/A	0	0
Total Non-Personnel	**50,788**	N/A	N/A	**545**	**1,390**

4. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	30	0	30	5,564	107,370	112,934	N/A	N/A
Increases	6	0	3	752	50,788	51,540	1,151	2,092
Grand Total	**36**	**0**	**33**	**6,316**	**158,158**	**164,474**	**1,403**	**1,546**

5. Enhancement Categorized by Cyber BDR 23-39

Type of Agency Funding	NIST Framework Function	Funding Amount ($000)
Discretionary	Detect	$ 2,900
	Identify	$ 12,600
	M-22-16	
	Protect	$ 140,974
	Respond	$ 8,000
	Total Discretionary Funding	$ 164,474
Mandatory	N/A	$ -
	Total Mandatory Funding	$ -
	Grand Total	$ 164,474

6. Affected Crosscuts

The Cybersecurity crosscut is affected by this enhancement.

Item Name: **E.O. 14110 Implementation (Artificial Intelligence)**

Budget Decision Unit(s): Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions: 1 Agt/Atty 0 FTE 1 Dollars $2,460,000

Description of Item

The enhancement request of $2.5 million will provide resources to create a Department-level governance structure to ensure the adoption of Artificial Intelligence (AI) in a productive, secure, and achievable manner in accordance with Executive Order 14110, *Safe, Secure, and Trustworthy Development and use of Artificial Intelligence*. The nature of DOJ's law enforcement and litigation missions present numerous opportunities for the use of AI, but also requires proactive steps to ensure the public's rights and safety. In addition to developing a secure governance framework, the Department will implement secure cloud-based test environments to allow components to safely test AI use-cases that can provide informed feedback to support the overall governance process, providing a path to scale useful AI initiatives across workloads and organizations.

Justification

E.O. 14110 Implementation (Artificial Intelligence) – $2.5M; 1 position

Executive Order 14110 as well as the corresponding OMB Memorandum, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, focuses on strengthening the appropriate use of AI across several domains, including the criminal justice system, to provide increased innovation and capabilities while maintaining public trust and safety. Within 60 days of the receipt of implementing guidance, agencies are required to put an AI governance mechanism in place. This will require the DOJ to implement a consistent and cross-cutting AI governance mechanism at the Department level, in addition to taking positive steps to enable the expanded and thoughtful use of generative AI solutions. The DOJ will establish a centralized AI governance structure to coordinate AI issues across senior leadership, create a risk management framework to protect the public's rights and safety, provide reporting on the uses of AI, continuously evaluate AI solutions, and provide remedies for the improper use of AI. To enable consistent and informed use, the DOJ will also fund the implementation of AI test environments to allow Components to formulate, test and scale AI use cases to meet mission requirements. As many components across the DOJ currently lack the funding to address the requirements of the E.O., the enterprise test environments will allow organizations to learn about the technology, increase AI skills of existing staff, share lessons learned across the enterprise, and provide feedback to the governance mechanism in a secure and well-defined environment. As solutions continue to mature and proceed through the governance process, the DOJ will leverage cloud-based platforms to scale successful solutions.

Funding is required to establish and secure the cloud-based AI platforms, purchase initial licenses and consumption activity, train users and technical staff on the technology, and provide feedback to the governance mechanism. Resources will be required to administer the platform environments and provide day-to-day administration of the governance process. As components mature their AI use cases and through the governance process, they will migrate their AI solutions from the test environment to a production environment, at which point they will assume the funding responsibilities for sustaining their use cases under new or existing program funding outside the scope of this budget request.

Impact on Performance

To capitalize on the extraordinary capabilities of AI in a responsible and secure manner, the Department must establish mechanisms that adhere to the principles outlined in EO 14110. As this is an emerging executive order mandate, the DOJ currently lacks the capacity and funding to meet the intent of the E.O. The funding will support the development of technical support prescribed by the E.O. to enable the consistent and appropriate use of generative AI within the timelines prescribed. The support will also assist the DOJ Components by providing them with a secure environment and a consistent governance process to safely test their AI use cases for law enforcement, litigation support and administrative processes. This funding will also provide a secure path to broaden AI adoption in an appropriate manner consistent with maintaining public trust.

Funding

7. Base Funding

FY 2023 Enacted				FY 2024 President's Budget				FY 2025 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	0	0	0	0	0	0	0	0	0

8. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Info Technology Mgmt (2210)	145	1	283	153	14	153	14
Total Personnel	**145**	**1**	**283**	**153**	**14**	**153**	**14**

9. Non-Personnel Increase/Reduction Cost Summary

The enhancement request includes contractual and advisory services to provide ongoing information technology development and associated software support.

Non-Personnel Item	FY 2025 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Contract Labor	1,519	N/A	N/A	33	85
Software	796	N/A	N/A	0	0
Total Non-Personnel	**2,315**	N/A	N/A	**33**	**85**

10. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	0	0	0	0	0	0	N/A	N/A
Increases	1	0	1	145	2,315	2,460	186	99
Grand Total	**1**	**0**	**1**	**145**	**2,315**	**2,460**	**186**	**99**

11. Affected Crosscuts

None.

Item Name: **National Law Enforcement Accountability Database**

Budget Decision Unit(s): Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions 2 Agt/Atty FTE 1 Dollars $10,000,000

Description of Item

The enhancement request of $10 million and 2 positions will provide resources for establishing a National Law Enforcement Accountability Database in accordance with section 5 of Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*.

Justification

National Law Enforcement Accountability Database (NLEAD) – $10.0 million, two positions

Executive Order 14074 (EO 14074) is focused on increasing public trust and enhancing public safety and security by encouraging equitable and community-oriented policing. As mandated in the EO 14074, the Department must establish and administer the National Law Enforcement Accountability Database (NLEAD), ensuring compliance with the requirements of the Privacy Act of 1974 (as amended), 5 U.S.C. § 552a, and other relevant sections with the legal requirements. This includes providing appropriate due process protections for the federal law enforcement officers included in the database. NLEAD will serve as a centralized repository of official records documenting instances of law enforcement officer misconduct as well as commendations and awards. The database must be established to comply with the Privacy Act, the Federal Information Security Modernization Act, other applicable laws, and due process. Given the size and complexity of this task, funding is necessary to design, build, and continue administering the NLEAD. This funding will be used to develop and maintain the technical infrastructure required for storing, organizing, and securing the data in the database. Additionally, adequate funds are necessary for hiring and training personnel responsible for managing the database, coordinate with all federal law enforcement agencies, manage the identity and access for the database, verifying the accuracy of the information, and ensure compliance with privacy and data protection regulations.

As of February 2024, the NLEAD has met initial system milestones with 70% of agencies having contributed data and the remaining agencies slated to complete their initial data uploads by May 2024. Moving forward, additional funding is required to automate and scale the processes needed to manage user access, provide regular reports, and process data change requests. Additionally, in order to fulfill the mandate of the E.O., the NLEAD will require a substantial investment in identity proofing and user access licensing to support State, Local, Tribal and Territorial (SLTT) access to the system. It is important to note that the technical and

program management costs will recur as maintenance of the system and the policy process to sustain user adoption will continue.

NLEAD will require investment into software, infrastructure and cloud services associated with developing a new application. Contractor support will be necessary to provide end user support, access management, programmatic engagement activities, privacy compliance, and response center staffing. Initially, resources will be focused on development and then transition to coordination and integration with all federal law enforcement agencies. The funding for NLEAD will also cover the associated Identity, Credential and Access Management (ICAM) cost that will provide secure access as well as the data management and movement requirements among partners.

Impact on Performance

To stand up the mandated database and provided sufficient support for operation, the Department must receive the requested enhancements. As this is an emerging executive mandate, the Department lacks the full capability to create this repository without additional funds and resources, prohibiting the Department from being compliant with Executive Order 14074.

Funding

1. **Base Funding**

FY 2023 Enacted				FY 2024 President's Budget				FY 2025 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	0	0	0	0	0	0	0	0	0

2. **Personnel Increase Cost Summary**

Type of Position/Series	FY 2025 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				2nd Year	3rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Info Technology Mgmt (2210)	270	2	264	147	20	295	40
Total Personnel	**270**	**2**	**264**	**147**	**20**	**295**	**40**

3. Non-Personnel Increase/Reduction Cost Summary

The enhancement request includes contractual and advisory services to provide ongoing information technology development and associated software support.

Non-Personnel Item	FY 2025 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Contract Labor	8,730	N/A	N/A	175	437
Software	1,000	N/A	N/A	-50	-150
Total Non-Personnel	**9,730**	N/A	N/A	**125**	**287**

4. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	0	0	0	0	0	0	N/A	N/A
Increases	2	0	1	270	9,730	10,000	272	287
Grand Total	**2**	**0**	**1**	**270**	**9,730**	**10,000**	**272**	**327**

5. Affected Crosscuts

None.

VI. Exhibits