U.S. DEPARTMENT OF JUSTICE

Justice Information Sharing Technology

FY 2024 PERFORMANCE BUDGET

Congressional Justification

Attachment A

Table of Contents

I. Overview

II. Summary of Program Changes

III. Appropriations Language and Analysis of Appropriations Language

IV. Program Activity Justification

A. Justice Information Sharing Technology
1. Program Description
2. Performance Tables
3. Performance, Resources, and Strategies

V. Program Increases by Item

A. Cybersecurity Posture Enhancements

VI. Exhibits

I. Overview for Justice Information Sharing Technology

The Fiscal Year (FY) 2024 Justice Information Sharing Technology (JIST) request totals $193.6 million and includes 56 authorized positions and 52 full-time equivalents (FTE). This budget represents an increase of $55.6 million from the FY 2023 Enacted Budget and includes funds for current services adjustments and one program enhancement.

JIST funding supports Department of Justice (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 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 2024, 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.

DOJ will also support enterprise IT initiatives by continuing the strategy enacted in the FY 2014 budget of reinvesting cost savings. Through this strategy, the Department's FY 2024 budget requests the authority to transfer up to $40.0 million from DOJ components and that these funds remain available to the OCIO until expended. These funds will advance initiatives in IT modernization and allow DOJ to invest intelligently 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	**Transition from traditional network access monitoring to identity-based access for applications and data (zero trust); 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**	**$55,057**	**16**

III. Appropriations Language and Analysis of Appropriations Language

Justice Information Sharing Technology

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, *$193,630,000* 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)
2022 Enacted	33	32	$38,000
2023 Enacted	50	42	$138,000
Adjustments to Base and Technical Adjustments	0	7	$573
2024 Current Services	50	49	$138,573
2024 Program Increases	6	3	$55,057
2024 Program Offsets	0	0	$0
2024 Request	56	52	$193,630
Total Change 2023-2024			**$55,630**

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 DOJ's overall strategic goals and objectives. JIST also allows the OCIO to provide oversight and execution of DOJ IT projects in alignment with Department architectures and sound management principles. The FY 2024 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 DOJ's cybersecurity posture remains a top priority for the Department and its leadership, as 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, personnel, hardware, and software costs continue to rise, 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 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 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.

DOJ will also 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 DOJ resources to access applications and data while providing protection from targeted phishing attacks. As part of its ZTA transition, 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 DOJ internet gateways. The JSOC continues to identify increases in email, cloud, and mobile device attacks. Adversaries have become increasingly automated and complex, requiring 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 DOJ embraces new technologies, the OCIO must ensure secure deployment to safeguard data while supporting DOJ operational missions.

The DOJ continues to invest in infrastructure modernization across its 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 intends to establish 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 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 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 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 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 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 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 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 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 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 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 DOJ offices regardless of location or device. DOJ is nearing completion of transitioning all DOJ Components to a common email system by July 2023, The next phases will deploy technologies to ensure real-time data sharing and enhanced collaboration. These will 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 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) and the Department Investment Review Board (DIRB), which allows the 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, Managing Information as a Strategic Resource.

Oversight of the DOJ IT environment by the CIO is vital given the role of technology in supporting 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, as well as evaluate IT budget enhancement requests, among other responsibilities. This includes projects and services related to High Value Asset system. The DIRC directly supports the responsibilities of the DIRB. 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 DOJ mission requirements. By creating partnerships with 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 DOJ user experiences while ensuring alignment with 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 cause program risks, delays, and cost increases.

By applying human-centered design principles to understand DOJ's 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												
RESOURCES ($ in thousands)			**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
			FY 2022		**FY 2022**		**FY 2023**		**Current Services Adjustments and FY 2024 Program Changes**		**FY 2024 Request**	
Total Costs and FTE (Reimbursable: FTE are included, but costs are bracketed and not included in totals)			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			32	38,000			42	138,000	10	55,630	52	193,630
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2022**		**FY 2022**		**FY 2023**		**Current Services Adjustments and FY 2024 Program Changes**		**FY 2024 Request**	
Program Activity			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			32	38,000			42	138,000	10	55,630	52	193,630
KPI: Output	1.2	Percent of Department websites reflecting U.S. Web Design System requirements and meeting best practices for plain language and user centered design	5%				20%		30%		50%	
KPI: Output	1.2	Percent of common data sets accessible amongst DOJ components.	2%				10%		10%		20%	

KPII: Output	2.4	Percent of confirmed cyber incidents to Department systems.	<.001%		<.001%	0	<.001%

*Denotes inclusion in the DOJ Quarterly Status Report and DOJ Annual Performance Plan.
*This table is required.

Note that the dollars and FTE presented on the Performance and Resources Table(s) must total to the relevant columns on all other exhibits. ***Reimbursable and other FTE should be included in the totals****, while reimbursable dollars should be shown in brackets as a non-add item.*

Please describe the data definition, validation, verification, and data limitations for the performance measures included in the performance and resources table

Strategic Objective	**PERFORMANCE MEASURE TABLE**					
	Decision Unit:					
	Performance Measures		**FY 2022**	**FY 2022**	**FY 2023**	**FY 2024**
			Target	**Actual**	**Target**	**Target**
	Key Performance Indicator	Percent of Department websites reflecting U.S. Web Design System requirements and meeting best practices for plain	5%		20%	50%

		language and user centered design.				
	Key Performance Indicator	Percent of common data sets accessible amongst DOJ components.	2%		10%	20%
	Key Performance Indicator	Percent of confirmed cyber incidents to Department systems.	<.001%		<.001%	<.001%

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

In FY 2024, 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. They also support 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 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:** Optimizing CEF and cloud operations through shared services and solutions, with an emphasis on prioritizing application rationalization 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 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, DIRB, CIO Council, and Federal IT Dashboard Report.

(3) Cybersecurity – Protect Critical Mission Assets

With threats to DOJ increasing in frequency and complexity, protecting 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 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, 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 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 $55,057,000

Description of Item

The enhancement request of $55.1 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*, and NSM-8, *National Security Memorandum: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, 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:

- Zero Trust Architecture for Unclassified Systems - $11,000,000; three positions
- Zero Trust Architecture for National Security Systems - $13,700,000; 0 positions
- Cybersecurity Event Logging - $30,357,000; three positions

Justification

Zero Trust Architecture for Unclassified Systems – $11.0 million, three 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. A transition to a "zero trust" approach to security provides a defensible architecture for this new environment. The Department plans to implement a ZTA, advanced endpoint detection and response, and phishing-resistant Multi-Factor Authentication (MFA). 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 DOJ 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 and will maintain the capability with this enhancement.

- 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 move away from traditional network access monitoring to identity-based access to applications and data. ZTA allows 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 provide necessary capabilities to monitor additional logs and alerts, further refining JSOC services to adapt to ongoing changes in the threat landscape.

- Multi-Factor Authentication/Encryption

  In alignment with OMB M-22-09, the Department is moving to a centralized identity provider and authentication model, eliminating the individual federated component trust model exploited in the SolarWinds incident and creating a universal, mandatory multi-factor authentication. Under this model, identities and application access will be managed centrally and individual users will be authenticated with OMB-mandated Personal Identity Verification (PIV). However, alternate strong, phishing-resistant MFA is required when personnel, such as our State and local partners, cannot use PIV. When a smartcard is not possible, the Department will use a combination of industry standards, such as FIDO2 (access security) 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 our National Security Systems (NSS) infrastructure. The lack of a comprehensive ZTA for NSS puts the Department's most sensitive classified data and mission at risk of falling behind in defensive capabilities. Strong protection of NSS is critical to mission-essential activities through information sharing networks such as 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.

Cybersecurity Event Logging Enhancement – $30.4 million, three positions

Major incidents (i.e., SolarWinds) underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on 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 across all the Department's approximately 200,000 devices, which increases the data types and resources from seven terabytes (TB) per day to 81 TB per day. The DOJ will also need to increase the duration of historical log data from 12 months to 30 months. 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 OCIO is estimating a significant increase in the cost for storage, technical capabilities, as well as additional full-time resources, to meet all requirements.

Additionally, 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 within the trillions of events ingested into the JSOC each day, a feat that would be impossible without these enhancements.

Impact on Performance

The evolving threat landscape has made traditional perimeter-based network defense obsolete, as 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 will require software-defined policies and permit dynamic decisions, which will allow the OCIO to adjust permissions and enable increased access to applications when needed, but also remove and protect access when inconsistent user behavior exists. ZTA addresses these areas via central Identity Provider (IdP) identity-based access control through a broker, and advanced endpoint monitoring with EDR. By evolving our security and implementing a comprehensive ZTA, the Department will update its security protocols to secure data and access to reduce the risk of another SolarWinds type of incident.

The Department must be a reliable partner in the protection of the nation's most sensitive information. Perimeter-based security models are becoming obsolete, with malicious attacks

focused on identity and end-users to gain access to sensitive systems. The DOJ is implementing modern Software Defined Perimeter technology using identity-centric intelligence, to secure NSS access. With more robust frameworks in place, the Department reduces the risks of losing essential access to sensitive networks and data.

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. The additional resources are necessary for the Department to avoid the risk of implementing cloud services that become avenues for exploitation by adversaries.

Current levels of event logging are neither 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. With significant resource investment, the Department can deploy sufficient monitoring, improve its understanding of ongoing cyber threats and attacks, and develop comprehensive data enabling critical incident response decisions. The investment in logging will improve the Department's ability to scope attacks within the trillions of events ingested into the JSOC each day.

With the requested program enhancements, the Department can deploy 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 2022 Enacted				FY 2023 Enacted				FY 2024 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
4	0	4	$12,274	21	0	14	$112,078	21	0	21	$113,112

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Info Technology Mgmt (2210)	$802	6	$262	$128	$5	$768	$32

Type of Position/Series	FY 2024 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Total Personnel	**$802**	**6**	**$262**	**$128**	**$5**	**$768**	**$32**

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 2024 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Contract Labor	$5,300	N/A	N/A	$0	$0
Software	$46,955	N/A	N/A	$0	$0
Hardware	$2,000	N/A	N/A	-$1,333	$0
Total Non-Personnel	**$54,255**	**N/A**	**N/A**	**-$1,333**	**$0**

4. Justification for Non-Personnel Annualizations

The software items included in this request have trended towards an annual subscription model over on-premise license purchase for most competitive vendors. The requested annualization for the request is the total cost to provide software licenses and support services for each initiative to allow and support continuous upgrades to the software subscriptions.

5. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2025 (net change from 2024)	FY 2026 (net change from 2025)
Current Services	21	0	21	$5,411	$107,701	$113,112	N/A	N/A
Increases	6	0	3	$802	$54,255	$55,057	- $565	$32
Total	**27**	**0**	**23**	**$6,213**	**$161,956**	**$168,169**	**-$565**	**$32**

6. Enhancement Categorized by Cyber BDR 22-39

Type of Agency Funding	NIST Framework Function	Funding Amount ($000)
Discretionary	Detect	$4,280
	Identify	$13,290
	M-22-16	$5,370
	Protect	$136,839
	Respond	$8,390
	Total Discretionary Funding	**$168,169**
Mandatory	N/A	$0
	Total Mandatory Funding	**$0**
	Grand Total	**$168,169**

VI. Exhibits