U.S. DEPARTMENT OF JUSTICE

Justice Information Sharing Technology

FY 2027 PERFORMANCE BUDGET
CONGRESSIONAL SUBMISSION

Attachment A

Table of Contents

I. Overview for Justice Information Sharing Technology

The Fiscal Year (FY) 2027 Justice Information Sharing Technology (JIST) request totals $149 million and includes 49 authorized positions and 49 full-time equivalents (FTE). This Budget represents an increase of $110.5 million from the FY 2026 Enacted Budget ($38.5 million). This includes $206,000 for current services adjustments and $110.3 million for critical cybersecurity program increases.

JIST funding supports the Department of Justice (the DOJ, Department) enterprise investments in critical enterprise cybersecurity services and information technology (IT) modernization. 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 cybersecurity strategy, IT strategy, and enterprise architecture as well as in compliance with the statute requirements of the Federal Information Technology Acquisition Reform Act (FITARA). CIO oversight of the DOJ IT environment is critical given the level of dependence on the IT infrastructure and cybersecurity posture inherent to conducting legal, investigative, and administrative functions throughout the Department. This submission continues to help move the Office of the Chief Information Officer (OCIO) toward leveraging industry strategic leaders and partners to deliver advanced services DOJ-wide.

II. Summary of Program Changes

Item Name	Description	Positions	FTE	Amount ($000)	Page
Zero Trust Architecture (ZTA) for Unclassified Systems	Support department-wide cybersecurity improvements, including unified identity-based access for applications and data, real-time cloud security monitoring, and increased event logging capacity.	0	0	$44,274	11
National Security Systems (NSS) Enhancements	Zero Trust Architecture (ZTA) solution and NSS cybersecurity updates, outside of FBI systems.	0	0	$66,060	15

III. Appropriations Language and Analysis of Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, *$149,000,000* 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
2025 Enacted	50	40	$38,460
2026 Enacted	49	43	$38,460
Adjustments to Base and Technical Adjustments	0	6	$206
2027 Current Services	49	49	$38,666
2027 Program Increases	0	0	$110,334
2027 Request	49	49	$149,000
Total Change 2026-2027	**0**	**0**	**$110,540**

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. The DOJ CIO leverages JIST resources to drive continual advances in the Department's cybersecurity architecture, systems and processes to ensure DOJ enterprise and information resources are resilient and secure against a continually evolving threat landscape. 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 2027 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. Enterprise Cybersecurity

Enhancing the DOJ's cybersecurity posture remains a top priority for the Department, 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, architectural framework 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. The following program investments will enable DOJ to continue operating and maturing its IT enterprise, cybersecurity architecture and capabilities, enhancing threat detection, improving incident response, and securing access control.

(1) Enterprise 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 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 enterprise 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 to access applications and data while providing protection from targeted phishing attacks. As part of its ZTA, the DOJ continues operating enterprise endpoint detection and response, phishing-resistant Multi-Factor Authentication (MFA), centralized authentication, cloud native network access, and centralized logging.

(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. As the DOJ embraces new technologies and modernizes, 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 provides 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 significantly improves the security posture of the DOJ networks and

applications, while simultaneously allowing for greater information sharing between the DOJ components, Federal 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 and mitigation (CDM), and enterprise visibility, 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:

- Information assurance analysis supporting enterprise cybersecurity posture and cybersecurity supply chain risk management;
- Automated asset, configuration, and vulnerability management;
- Networks and systems scanning for anomalies; and
- Dashboard reporting for executive awareness and risk-based decision-making in near real-time.

The program continuously evolves to address the changing cyber-threat landscape, leveraging advanced expands on the suite of analytics to provide the DOJ analysts and leadership with consistent and reliable visibility of mission-enabling systems' security. DOJ's High Value Assets remain a critical focus of continuous processes and tooling refinement to help identify, assess, and remediate vulnerabilities.

b. IT Transformation and Innovation Engineering

The OCIO is committed to evolving the DOJ's IT environment by driving toward shared commodity infrastructure services, simplified design and implementation of tools, and harnessing innovative modern solutions to advance the mission. These efforts allow the DOJ to shift from legacy and custom government-owned solutions to advanced industry-leading offerings at competitive pricing. 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. As such, the OCIO will continue investing in the following initiatives.

(1) Data Center Transformation and Network Optimization

The Department is committed to achieving "smaller and smarter" data center infrastructure with improved operational efficiency and overall cost savings. 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. 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. Additionally, OCIO will focus on gaining enterprise-wide efficiencies through emerging compute and networking

technologies that offer more cost effective, scalable performance that simplifies service delivery.

(2) Innovation and Technology

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 and aid mission delivery. OCIO's focus remains on accelerating the replacement of legacy, burdensome, often duplicative technologies with resilient, cloud-based capabilities that underpin modernized, streamlined, cost efficient and secure operations. The OCIO evaluates the maturity of innovative technologies and organizational readiness for incorporation into the enterprise,, such as identifying use cases where artificial intelligence, machine learning, or advanced analytics can accelerate mission outcomes.

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), as well as the prioritization of enterprise solutions and shared services. 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 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 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, as well as continually reinforcing the consolidation of services and standardization of systems to improve efficiency, reduce risk, and eliminate unnecessary duplication.

V. Program Increases by Item

Item Name: **Zero-Trust Architecture for Unclassified Systems**

Budget Decision Unit(s): Justice Management Division

Organizational Program: Justice Information Sharing Technology (JIST)

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $44,274,000

Description of Item

Resources are requested to enhance the Department's Zero-Trust Architecture (ZTA) for unclassified systems. This funding will support department-wide cybersecurity improvements, including unified identity-based access for applications and data, real-time cloud security monitoring, and increased event logging capacity. These enhancements aim to improve information sharing, network segmentation, and overall cybersecurity posture in response to several Executive Orders focused on strengthening national cybersecurity, eliminating information silos, and enabling secure, enterprise-wide data sharing. No new positions are requested with this funding.

Justification

The massive SolarWinds breach in 2020, the most sophisticated nation-state supply chain attack ever recorded, helped precipitate a reframing of Federal cybersecurity away from the "castle and moat" approach towards today's dynamic "always verify, never trust" ZTA model. Accordingly, DOJ has heavily relied on the JIST appropriation to implement and sustain ZTA capabilities on its unclassified systems. These investments align with Executive Order 14306 and the administration's cybersecurity strategy.

JIST funding was cut by $108 million in FY 2024 enacted appropriations. Enacted funding levels over the past three years are below the level required to cover DOJ's over 275,000 endpoints and approximately 160,000 users. Additional funding is needed to continue progress on the Department's cohesive zero trust model to support the Department's ability to counter advancing threats from nation-state actors and fully implement cross-component information sharing and collaboration.

The Department requires additional resources to pay for cybersecurity software licenses and engineering, which support the current infrastructure and provide a secure environment for DOJ's information and technology assets and for its users.

Impact on Performance

As cyber threats become more and more sophisticated, the current funding levels impact the Department's current defenses and constrain its ability to adapt to evolving threats. Without full ZTA implementation, the Department's cyber risk exposure and its susceptibility to major

breaches and catastrophic cyber incidents compromising DOJ's capacity to safeguard sensitive law enforcement, national security, and mission-critical systems or infrastructure increases.

(1) Unified Identity Provider

As part of the post-SolarWinds remediation, the Department has been focused on deploying a centralized identity provider (IdP), a critical initiative aimed at strengthening access controls and reducing the Department's identity attack surface. FY 2024's cut to JIST has necessitated a reduction in labor expenditures supporting this unification effort, and, without this program increase, will force the termination of the requisite IdP licenses, halting the unified identity pillar of the Department's modern cybersecurity architecture. Rolling back the deployment will force the Department to move applications back to the previous state, one which allows attackers that successfully gain unauthorized, undetected access to DOJ systems to move laterally within the environment to escalate privileges or exfiltrate sensitive data.

(2) Zero Trust Network Broker

The Department has initiated a cloud-based zero trust network broker platform implementation to enhance the Department's network security and to align with the network pillar of the Cybersecurity and Infrastructure Security Agency's zero trust maturity model. Network configuration policies are in place to limit lateral movement of traffic, ensuring that only authenticated users and devices can access specific applications. Without this program increase, the Department will have to discontinue the Zero Trust network broker initiative entirely, preventing DOJ's full implementation of cross-component information sharing and collaboration as well as reverting to traditional Virtual Private Networks (VPN) that lack the advanced continuous monitoring and granular access controls needed to protect the Department from sophisticated cyber threats and breaches.

(3) Endpoint Detection and Response (EDR) and Mobile Threat Detection (MTD)

To elevate cybersecurity protection across DOJ devices and enable enterprise visibility, DOJ has deployed a modern cloud based EDR and MTD solution to over 275,000 of the Department's workstations, laptops, servers, and mobile devices. The enhanced visibility enabled by the DOJ EDR and MTD deployment is essential for detecting, investigating, and responding to advanced persistent threats on the network. Without this program increase, the Department will be in the position of having to discontinue its EDR and MTD capabilities. The removal of EDR and MTD will curtail the Department's ability to identify and mitigate cyber threats like ransomware and malware in real time and diminish the availability of the telemetry data required to proactively hunt for suspicious activity.

Funding

Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
24	0	23	27,817	24	0	19	31,682	25	0	25	31,888

Non-Personnel Increase/Reduction Cost Summary

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

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Contract Labor	8,210	N/A	N/A	411	519
Software	36,064	N/A	N/A	2,885	2,476
Total Non-Personnel	**44,274**	**N/A**	**N/A**	**3,296**	**2,995**

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	25	0	25	8,494	23,394	31,888	0	0
Increases	0	0	0	0	44,274	44,274	2,432	2,620
Grand Total	**25**	**0**	**25**	**8,494**	**67,668**	**76,162**	**2,432**	**2,620**

Item Name: **National Security Systems (NSS) Enhancements**

Budget Decision Unit(s): Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions 0 Agt/Atty 0 FTE 0 Dollars $66,060,000

Description of Item

Resources are requested to implement a Zero-Trust Architecture (ZTA) solution and upgrades for National Security Systems (NSS) of the Department, outside of FBI systems. Zero Trust is a cyber framework that assumes no user or system is inherently trusted and requires continuous verification of identity, access, and device before granting access. With ZTA and new capabilities, the Department's NSS will be equipped to continuously verify users, enforcing strict access policies that block unauthorized communication, thereby reducing the potential spread of threats or risk of breaches impacting national security systems and data. No new positions are requested with this funding.

Justification

Unlike one-time authentication models, a Zero Trust solution will provide continuous verification of users and devices, ensuring that every access request is evaluated in real time. This is especially crucial for NSS and classified systems as they hold the nation's most sensitive information.

Impact on Performance

Adversaries today focus on exploiting lateral movement in their aim to gain access to the Nation's most critical applications and systems. Without the requested program increase, the Department will lack the full capability to successfully defend against our cyber enemies' advanced threats designed to disrupt the Department's missions and compromise sensitive data. The investment is justified by the reduced breach potential and the need to maintain Federal compliance.

Funding

Base Funding

FY 2025 Enacted				FY 2026 Enacted				FY 2027 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	66,060

Non-Personnel Increase/Reduction Cost Summary

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

Non-Personnel Item	FY 2027 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Contract Labor	2,614	N/A	N/A	131	138
Software	63,446	N/A	N/A	-51,300	607
Total Non-Personnel	**66,060**	**N/A**	**N/A**	**-51,169**	**745**

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2028 (net change from 2027)	FY 2029 (net change from 2028)
Current Services	0	0	0	0	0	0	N/A	N/A
Increases	0	0	0	0	66,060	66,060	-51,169	745
Grand Total	**0**	**0**	**0**	**0**	**66,060**	**66,060**	**-51,169**	**745**