U.S. DEPARTMENT OF JUSTICE

Justice Information Sharing Technology

FY 2023 PERFORMANCE BUDGET

Congressional Justification

U.S. Department of Justice
Justice Information Sharing Technology

FY 2023 Performance Budget
Congressional Justification

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. Strengthening Cybersecurity
B. Supply Chain Risk Management

VI. Exhibits

A. Organizational Chart
B. Summary of Requirements
B. Summary of Requirements by DU
C. FY 2023 Program Increases/Offsets by Decision Unit
D. Resources by Department of Justice Strategic Goal and Objective
E. Justifications for Technical and Base Adjustments
F. Crosswalk of FY 2021 Availability
G. Crosswalk of FY 2022 Availability
H-R. Summary of Reimbursables Resources
H-S. Summary of Sub-Allotments and Direct Collections Resources
I. Detail of Permanent Positions by Category
J. Financial Analysis of Program Changes
K. Summary of Requirements by Object Class
L. Status of Congressionally Requested Studies, Reports, and Evaluations (Not Applicable)

I. Overview for Justice Information Sharing Technology

The Fiscal Year (FY) 2023 Justice Information Sharing Technology (JIST) request totals $153.1 million and includes 50 authorized positions and 43 full-time equivalent (FTE). This budget represents an increase of $40.0 million from the FY 2022 President's Budget and includes funds for current services adjustments and two program enhancements (17 authorized positions, 10 FTE).

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 2023, the JIST appropriation will fund OCIO's continuing efforts to provide innovative technologies and services in support of the Attorney General's Strategic Plan for FY 2022-2026 and the President's Management Agenda. 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 2023 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
Supply Chain Risk Management	**Resources to improve the Department's supply chain risk management with a focus on providing insight into the source and potential vulnerability of critical systems and technology.**	**2**	**2**	**$500**	**14**
Strengthening Cybersecurity	**Resources to remediate the SolarWinds incident and address other opportunities to bolster cybersecurity defense and resilience through 1) data management and application security and 2) cyber workforce development and retention.**	**15**	**8**	**$40,000**	**16**

III. Appropriations Language and Analysis of Appropriations Language

Appropriations Language

Justice Information Sharing Technology

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, *$153,057,000* 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
2021 Enacted	33	32	34,000
2022 Annualized CR	33	32	34,000
2022 Rebaseline Adjustment	0	0	79,024
Adjustments to Base and Technical Adjustments	0	1	-467
2023 Current Services	33	33	112,557
2023 Program Increases	17	10	40,500
2023 Program Offsets	0	0	0
2023 Request	50	43	153,057
Total Change 2022-2023	**17**	**10**	**40,033**

***Justice Information Sharing Technology*- Information Technology Breakout (of Decision Unit Total)**	Direct Positions	Estimated FTE	Amount ($000)
2021 Enacted	33	32	34,000
2022 Annualized CR	33	32	34,000
2022 Rebaseline Adjustment	0	0	79,024
Adjustments to Base and Technical Adjustments	0	1	-467
2023 Current Services	33	33	112,557
2023 Program Increases	17	10	40,500
2023 Program Offsets	0	0	0
2023 Request	50	43	153,057
Total Change 2022-2023	**17**	**10**	**40,033**

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 2023 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) SolarWinds Incident Response

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 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 the detection of and response to attacks and limit its impact.

Endpoint Detection and Response

DOJ is implementing 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 response to security incidents and alerts. Device protection platforms integrate machine-learning, behavioral analytics, and anomaly detection to provide a more proactive approach to safeguarding endpoints, regardless of location or networks. A cloud-based option is best suited to support rapid deployment and scalability that provides comprehensive coverage for all DOJ laptops, mobile phones, desktops, and servers.

Cybersecurity Event Logging

DOJ is augmenting its logging capability to leverage cloud service provider Application Programming Interfaces to provide visibility into workloads, modifications, and enhanced response capabilities. DOJ is also implementing improved logging within the Department's cloud-based email system in order to

enable better detections of adversarial access and activity. Additionally, DOJ is working on a baseline solution that monitors the health and management of network devices and systems.

Cloud Security Upgrades

DOJ is enhancing its Office 365 (O365) licensing across all Department users to unlock additional security features that will provide better detections of adversarial access and activity within DOJ's O365 environment. The Department will also implement greater protection and increased monitoring for privileged access management, including a tiered administration approach to protect assets and limit administrative users.

Multi-Factor Authentication and Encryption

The Department is moving to a centralized identity provider and authentication model, which will eliminate the individual federated component trust model exploited in the SolarWinds incident, and creating a universal, mandatory multi-factor authentication. Under this new model, trust will be established at the individual user and device level using Office of Management and Budget (OMB)-mandated Personal Identity Verification (PIV) as the strong, second form factor, which requires DOJ to implement a secure certificate management system to effectively distribute and manage these authenticators. Additionally, leveraging the same authenticator, DOJ is implementing user level encryption, enhancing the ability to protect data while implementing the necessary capabilities for e-Discovery and records management.

Security Operations Center Maturation

In addition to the initiatives across logging, monitoring, and cloud visibility, the Justice Security Operations Center (JSOC) is implementing deceptive technology, or honeypots, as a technique to secure high value assets and disrupt threat actors' lateral movement by misleading or confusing the adversary through intentionally exposed decoy assets. The JSOC is planning and coordinating the implementation of zero-trust network capabilities to change the paradigm to enhance how DOJ applications are defended, accessed, and monitored.

(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 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 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 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 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 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 program supports mandates from OMB under the Data Center Optimization Initiative (DCOI) and

the federal cloud computing strategy. 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. The first phase of ECS, with a scheduled completion of all DOJ components by FY 2023, transitioned email to a common system, while 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. 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 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. 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 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 has initiated development of a DOJ Artificial Intelligence Strategy to maximize mission support.

2. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE												
Decision Unit: Justice Information Sharing Technology												
RESOURCES ($ in thousands)			**Target**		**Actual**		**Target**		**Changes**		**Requested (Total)**	
			FY 2021		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Changes**		**FY 2023 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	34,000 [38,840]	19	37,023 [18,970]	32	34,000 [38,840]	11	40,033 [10,660]	43	153,057 [49,500]
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2021**		**FY 2021**		**FY 2022**		**Current Services Adjustments and FY 2023 Program Changes**		**FY 2023 Request**	
Program Activity			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			32	34,000	19	37,023	32	34,000	11	40,033	43	153,057
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.	N/A		N/A		5%		15%		20%	
KPI: Output	1.2	Percent of common data sets accessible	N/A		N/A		2%		8%		10%	

		amongst DOJ components.					
KPI: Output	2.4	Percent of confirmed cyber incidents to Department systems.	N/A	N/A	<0.001%	0	<0.001%

Strategic Objective	**Performance**		**FY 2021**	**FY 2022**	**FY 2023**
			Actual	**Target**	**Target**
1.2	**Key Performance Indicator**	Percent of Department websites reflecting U.S. Web Design System requirements and meeting best practices for plain language and user centered design.	N/A	5%	20%
1.2	**Key Performance Indicator**	Percent of common data sets accessible amongst DOJ components.	N/A	2%	10%
2.4	**Key Performance Indicator**	Percent of confirmed cyber incidents to Department systems.	N/A	<0.001%	<0.001%

[N/A= Data Unavailable]

3. Performance, Resources, and Strategies

    a. Performance Plan and Report for Outcomes

In FY 2023, 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 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 through standardizing and simplifying technology, offering shared services and strategic sourcing, and leveraging IT governance to drive collective investment decisions.

The DOJ supports a number of 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: **Supply Chain Risk Management**

Budget Decision Unit: Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions 2 Agt/Atty 0 FTE 2 Dollars $500,000

Description of Item

The enhancement request of $500,000 and 2 positions will focus specifically on supply chain risk management and work in conjunction with the $40 million Strengthening Cybersecurity program enhancement request.

Justification

The OCIO will improve the Department's supply chain risk management with a focus on providing insight into the source and potential vulnerability of critical systems and technology to the Department. A key enhancement will include the development of new capabilities to analyze the cyber-specific risks associated with critical software vendors and to mitigate those threats. These efforts include: providing additional capacity to conduct supply chain risk assessments; increasing analytic capabilities; improving software security by leveraging software bill of material information; and implementing security requirements for critical software per the Executive Order 14028 and the Office of Management and Budget (OMB) Memorandum M-21-30, Protecting Critical Software Through Enhanced Security Measures.

Impact on Performance

The SolarWinds attack highlighted the risks associated with the Department's software supply chain. Executive Order 14028 requires Federal agencies to enhance their supply chain risk management programs to increase focus on software supply chain security. This enhancement is required for the Department to identify risks associated with our crucial software vendors that will impact every enclave and application within the enterprise.

Funding

Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 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

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs by Series ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Adjusted Cost		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Info Technology Mgmt (2210-2299)	2	$500	$510	$510	$500	$10	$0
Total Personnel	**2**	**$500**	**$510**	**$510**	**$500**	**$10**	**$0**

Non-Personnel Increase/Reduction Cost Summary

None requested.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	0	0	0	$0	$0	$0	$0	$0
Increases	2	0	2	$500	$0	$500	$10	$0
Grand Total	**2**	**0**	**2**	**$500**	**$0**	**$500**	**$0**	**$0**

Affected Crosscuts

The cyber crosscut will be affected by this request.

Item Name: **Strengthening Cybersecurity**

Budget Decision Unit: Justice Management Division

Organizational Program: Justice Information Sharing Technology

Program Increase: Positions 15 Agt/Atty 0 FTE 8 Dollars: $40,000,000

Description of Item

The enhancement request of $40.0 million and 15 positions will provide critical resources to continue the Department's cybersecurity-strengthening activities undertaken in FY 2022, to include continued remediation of the SolarWinds incident as well as addressing other opportunities to strengthen our cybersecurity defense and resilience. The additional personnel will plan implementation and deployment of technology to ensure the additional cybersecurity capabilities are developed and integrated throughout the Department.

In alignment with the President's Executive Order 14028 "Improving the Nation's Cybersecurity" (EO 14028), the Deputy Attorney General launched a 120-Day Comprehensive Cyber Review with DOJ component heads on May 19, 2021, to develop actionable recommendations to expand and enhance the Department's cybersecurity efforts. The OCIO will review and implement recommendations from three primary lines of effort: Deterrence, Disruption, and Accountability; Strengthening Our Defenses and Building Resilience; and Ensuring Our Workforce and Policies Reflect our Values and the Implications of Emerging Technologies, with notable focus on two initiatives:

- Data Management and Application Security - $34.0 million, 13 positions
- Cyber Workforce Development and Retention - $6.0 million, 2 positions

Justification

Data Management and Application Security

Per Executive Order 14028, Federal agencies must modernize cybersecurity, accelerate movement to secure cloud services, focus on protecting data in real-time, and secure the applications that interact with data. The OCIO will increase security operations capacity to improve automation, threat hunting, incident response, and monitoring; review policies and identify categories that should have encryption requirements, both for encryption in transit and at rest; address email encryption for records management and eDiscovery needs; and improve cloud security with a focus on securing data and applications.

The OCIO will expand the Department's penetration testing capabilities to include continuous penetration testing on all public facing services and add red team/blue team adversarial testing to emulate real world threats. These capabilities will enhance the ability of the DOJ to identify

vulnerabilities in systems that are not detectable through standardized vulnerability scanning tools and highlight the threats that are likely to impact the Department.

Applying User and Entity Behavioral Analytics (UEBA), the OCIO will focus on prevention of deliberate and intended actions, such as malicious exploitation; theft; destruction of data; and the compromise of networks, communications, or other information technology resources. A UEBA capability will allow the Department to take advantage of Artificial Intelligence (AI) capabilities to detect attacks within the trillions of events ingested into the Justice Security Operations Center each day, a feat that would be impossible without this capability.

As a result of the SolarWinds incident, the intelligence community requested the National Security Agency (NSA) to conduct a review across all network domain solutions for each security clearance level. Based on this review, the NSA developed the "Raise the Bar Strategy," which the OCIO will implement for cross-domain solutions to improve the Department's ability to address emerging threats and malicious insiders. These improvements are essential to protecting against threats targeting classified data and networks.

Cybersecurity Workforce Development

The recent increase in frequency and sophistication of cybersecurity threats and attacks has reinforced the criticality of hiring, developing, and retaining cybersecurity professionals with the technical skills necessary to defend the Department's mission albeit the limited availability of such professionals. To enhance DOJ's cybersecurity workforce, the OCIO will establish a Cybersecurity Retention Program to support the development and retention of its cybersecurity workforce. The OCIO will develop skill requirement and assessment programs that are consistent with cybersecurity workforce planning process and strategy to bolster and ensure baseline skillsets across the IT and cybersecurity staffs, including "live-fire" functional exercises and red team assessments. A major component of this program will include a cybersecurity functional exercise simulator where DOJ employees can experience the challenges and the fog of war associated with a major cyber breach in a controlled and safe environment.

Impact on Performance

The lack of a comprehensive data management and application security program will put millions of American's sensitive data and the Department's mission at risk. Programs like adversarial testing emulate advanced persistent threats to provide the DOJ with opportunities to identify how adversaries and bad actors might compromise our data and applications before it happens. This capability is critical for the OCIO to enhance the Department's ability and strategies in preventing and mitigating these threats.

In alignment with policy guidance of the Executive Order 14028, the use of secure cloud services provides an opportunity to improve the Department's security posture; however, as the world observed and learned through the follow-on activities from the SolarWinds incident, cloud services require customer cognizance of the security controls provided to them by the vendors. 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 additional resources are necessary for the Department to avoid the risk of implementing cloud services that become avenues for exploitation by adversaries. Additionally, the lack of a robust workforce development and retention program will impair the DOJ's ability to train and retain highly qualified IT and cybersecurity personnel and lead to a substandard cyber workforce.

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

Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
4	0	4	$8,512	4	0	4	$87,298	4	0	4	$87,298

Personnel Increase Cost Summary

Type of Position/Series	Positions Requested	Annual Costs by Series ($000)			FY 2023 Request ($000)	Annualizations ($000)	
		1st Year Adjusted Cost	2nd Year Adjusted Cost	3rd Year Adjusted Cost		FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Clerical and Office Svcs (0300-0399)	2	$415	$408	$408	$415	$-7	$0
Info Technology Mgmt (2210-2299)	13	$2,630	$2,680	$2,680	$2,630	$50	$0
Total Personnel	**15**	**$3,045**	**$3,088**	**$3,088**	**$3,045**	**$43**	**$0**

Non-Personnel Increase Cost Summary

The enhancement request includes contractual and advisory services to provide ongoing information technology development and associated software support. Specifically, the non-personnel increases included are:

- Data Management and Application Security
  - Contract labor support: $1.8 million
  - Advisory and consulting services: $13.3 million
  - Software licenses and subscriptions, including user and entity behavioral analytics tools and data storage, vulnerability and continuous penetration testing, and cross domain solution upgrades: $15.0 million
- Cyber Workforce Development and Retention
  - Contractor labor support: $250,000

- Advisory and consulting services: $2.8 million
- Software licenses and subscriptions, including cybersecurity functional exercises simulator: $3.8 million

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Contract Labor Support	$2,050	N/A	N/A	$0	$0
Advisory & Consulting Svcs	$16,105	N/A	N/A	$0	$0
Software	$18,800	N/A	N/A	$0	$0
Total Non-Personnel	**$36,955**	**N/A**	**N/A**	**$0**	**$0**

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 of the four initiatives to allow and support continuous upgrades to the software subscriptions.

Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2024 (net change from 2023)	FY 2025 (net change from 2024)
Current Services	4	0	4	$807	$86,491	$87,298	$0	$0
Increases	15	0	8	$3,045	$36,955	$40,000	$43	$0
Grand Total	**19**	**0**	**12**	**$3,852**	**$123,446**	**$127,298**	**$43**	**$0**

Affected Crosscuts

The cyber crosscut will be affected by this request.