U.S. Department of Justice
FY 2022 Congressional Justification

Justice Information Sharing Technology

U.S. Department of Justice

FY 2022 Performance Budget
OMB Submission

Table of Contents

I. Overview for Justice Information Sharing Technology (JIST)

The Fiscal Year (FY) 2022 Justice Information Sharing Technology (JIST) request totals $113.0 million and includes 33 full-time equivalent (FTE). JIST funding supports Department of Justice (DOJ) enterprise investments in IT modernization and critical cybersecurity requirements. This submission continues moving the Office of the Chief Information Officer (OCIO) toward leveraging industry strategic partners to deliver advanced services DOJ-wide.

As a centralized fund under the control of the DOJ 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's IT environment is critical given the level of dependence on the IT infrastructure and cybersecurity posture necessary to conduct legal, investigative, and administrative functions.

In FY 2022, 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 2018-2022 and 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 2022 budget requests a transfer of up to $40.0 million from DOJ components and requests that these funds remain available to augment JIST resources 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.

Electronic copies of the Department of Justice's Congressional Budget Justifications and Capital Asset Plan and Business Case exhibits can be viewed or downloaded from the Internet using the Internet address: https://www.justice.gov/doj/fy-2022-CJ

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Cybersecurity	**SolarWinds Incident Response**	**0**	**0**	**$78,786**	**16**
Total		**0**	**0**	**$78,786**	

III. Appropriations Language and Analysis of Appropriations Language

For necessary expenses for information sharing technology, including planning, development, deployment and departmental direction, $113,024,000 to remain available until expended: *Provided*, That the Attorney General may transfer up to $40.0 million to this account from funds made available to the Department of Justice in this Act for information technology, to remain

available until expended, for enterprise-wide information technology initiatives: *Provided further*, That the transfer authority in the preceding proviso is in addition to any other transfer authority contained in this Act: *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*

JIST	*Direct Pos.*	*Estimate FTE*	*Amount ($000)*
2020 Enacted	*33*	*33*	*33,875*
2021 Enacted	*33*	*32*	*34,000*
Adjustments to Base and Technical Adjustments	*0*	*0*	*0*
2022 Current Services	*33*	*32*	*34,238*
2022 Program Increase	*0*	*0*	*78,786*
2022 Request	*33*	*32*	*113,024*
Total Change 2021-2022	*0*	*0*	*79,024*

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 OCIO to provide oversight and execution of DOJ IT projects in alignment with Department architectures and sound management principles. The FY 2022 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.

1. 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 investigations, prosecution, and incarceration. 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 day-to-day security operations. While 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, DOJ will continue investing in the following programs to support DOJ components in protecting mission assets from today's dynamic threat environment.

a. Justice Security Operations Center (JSOC)

OCIO maintains and operates the JSOC, providing 24x7 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 on cybersecurity. As DOJ embraces new technologies, OCIO must ensure secure deployment to safeguard data, while supporting DOJ operational missions.

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

b. Identity, Credential, and Access Management (ICAM)

The goal of the ICAM program is 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-based authentication will significantly improve the security posture of the DOJ networks and applications, while simultaneously allowing for greater information sharing between DOJ components, other Federal Government agencies, and partners outside of the federal government.

The DOJ will enhance the ICAM program in the following ways:

- Identity services – Integrate DOJ applications with established identity and privileged account management solutions, allowing for automated access management, least privilege access enforcement, and reduced overall risk within the network; and
- Authentication services implementation – Implementation of authentication services to allow users and business partners to securely access DOJ data from various devices and platforms.

c. 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. In FY 2022, OCIO will implement a program to improve the security posture of

DOJ's High Value Assets, including new processes and tools to help identify, assess, and remediate vulnerabilities at the enterprise level.

d. 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.

To achieve the intent of the Insider Threat Full Operating Capability Goal, DOJ must have the capacity to detect patterns and correlated indicators across multiple types of information (e.g., human resources, information assurance, security, and counterintelligence). Having this capacity can lead to preventing (or mitigating) threats and adverse risks to the security of the United States.

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.

e. Continuous Diagnostics and Mitigation (CDM)

The CDM Program, centrally managed by 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.

2. IT Transformation

IT transformation is an ongoing commitment to evolve DOJ's IT environment by driving toward shared commodity infrastructure services and seeking simplified design and implementation of tools to advance the mission. These efforts will 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.

a. Joint Automated Booking System (JABS) / Civil Applicant System (CAS) Technology Modernization

OCIO provides biometric identity services to DOJ components and other federal and tribal agencies via the Joint Automated Booking System (JABS) and Civil Applicant System (CAS). To reduce security exposure and lower the cost of ownership, OCIO is replacing legacy systems with a modern, cloud-hosted solution. The new system integrates services into a single, modernized system and eliminates the need for customers to invest individually.

b. 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 the Office of Management and Budget (OMB) under the Data Center Optimization Initiative (DCOI) and the federal cloud computing strategy.

DOJ will continue to focus on consolidation activities by optimizing CEF operations through new processes and tools, migrating systems to cloud environments, and performing an application rationalization activity expected to not only achieve cost savings, but also simplify end-user experience and customer service. Overall, DOJ plans to consolidate 110 data centers to two CEFs.

c. Email and Collaboration Services (ECS)

The DOJ was one of the first large, federated 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 transitioned email to a common system (with the last two DOJ components scheduled for completion in FY 2021 and FY 2022), 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.

3. IT Architecture and Oversight

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. OCIO provides support to a wide-range of IT planning, governance, and oversight processes such as IT investment management and Capital Planning and Investment Control (CPIC), as well as the Department Investment Review Council (DIRC) and Department

Investment Review Board (DIRB), which allow 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 Federal Information as a Strategic Resource).

Oversight of the DOJ's 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 covering federal information technology 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 CFO's overall budget guidance, which is published each year and is coordinated with the formal Spring Call budget formulation process.
- 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.

OCIO also leverages the DIRC, made up of key DOJ and component executives, to monitor and support major and high visibility IT projects and services, as well as evaluate IT budget enhancement requests, among other responsibilities. The DIRC directly supports the responsibilities of the Department Investment Review Board. 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-level to develop solutions addressing mission and business needs.

4. Innovation Engineering

OCIO facilitates adoption of new and innovative technologies to support DOJ mission requirements. By creating partnerships with DOJ components, federal agencies, and industry for the exploration of these new technologies, OCIO is responsible for leading the ideation, design, planning, and execution of enterprise-wide IT innovations to enhance DOJ user experiences, while ensuring alignment with DOJ architectures and strategic priorities. 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 risk, delays, and cost increases.

By applying human-centered design principles to understand DOJ operational needs, 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, 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: JMD/OCIO/Justice Information Sharing Technology (JIST)												
RESOURCES			**Request**		**Actual**		**Projected**		**Changes**		**Requested (Total)**	
			FY 2020		**FY 2020**		**FY 2021**		**Current Services Adjustments and FY 2022 Program Changes**		**FY 2022 Request**	
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)			**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
			33	33,875 [53,323]	20	36,327 [53,323]	24	34,000 [38,840]	0	79,024 [0]	32	113,024 [28,250]
TYPE	**STRATEGIC OBJECTIVE**	**PERFORMANCE**	**FY 2020**		**FY 2020**		**FY 2021**		**Current Services Adjustments and FY**		**FY 2022 Request**	
			FTE	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**	**FTE**	**$000**
Program Activity			33	33,875 [53,323]	20	36,327 [53,323]	24	34,000 [38,840]	0	79,024 [0]	32	113,024 [28,250]
Performance Measure:	**1.2**	**Ensure IT systems are certified and accredited**	**100%**		**100%**		**100%**		**N/A**		**100%**	
Performance Measure:	**4.4**	**Number of DOJ systems moved to the cloud (ECS & Data Center only)**	**4**		**4**		**0**		**N/A**		**1**	
Data Definition, Validation, Verification, and Limitations: INFORMATION REQUIRED *Use this section to discuss data terms, data sources, how the information is collected, how the information is verified, and data limitations to include how well the indicator measures performance in this area.*												

Strategic Objective	PERFORMANCE MEASURE TABLE									
	Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)									
	Performance Report and Performance Plan Targets		FY 2016	FY 2017	FY 2018	FY 2019	FY 2020		FY 2021	FY 2022
			Actual	Actual	Actual	Actual	Target	Actual	Target	Target
1.2	Performance Measure	Ensure IT systems are certified and accredited	100%	100%	100%	100%	100%	100%	100%	100%
4.4	Performance Measure	Number of DOJ systems moved to the cloud (ECS & Data Center only)	N/A	N/A	14	5	4	4	0	1
	N/A = Data unavailable									

3. Performance, Resources, and Strategies

a. Performance Plan and Report for Outcomes

JIST-funded programs support the Department of Justice Strategic Plan for FY 2018-2022, which seeks to advance, protect, facilitate, and serve DOJ missions, by providing enterprise IT infrastructure and secure environments necessary to conduct national security, legal, investigative, and administrative functions. The FY 2018 – 2022 DOJ Strategic Goals are:

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

Specifically, JIST supports Strategic Objective 1.2 – Combat cyber-based threats and attacks; and Objective 4.4 – Achieve management excellence.

DOJ's IT Strategic Plan for FY 2019 – 2021 provides specific details on OCIO's approaches to transform IT and meet the objectives outlined in the Department of Justice Strategic Plan for 2018 - 2022 and the President's Management Agenda.

The FY 2019 – 2021 DOJ IT Strategic Goals are:

- DOJ IT Strategic Goal 1: Continuously Improve Service Delivery
- DOJ IT Strategic Goal 2: Effectively Invest in Technology
- DOJ IT Strategic Goal 3: Protect Critical Mission Assets
- DOJ IT Strategic Goal 4: 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 transforming business processes, as well as prioritizing investments in enterprise mission and cybersecurity.

b. Strategies to Accomplish Outcomes

i. IT Transformation – Continuously Improve Service Delivery (Goal 1)

As a provider of high-performing, resilient, and efficient services supporting DOJ's missions, DOJ must transform the delivery of current and new IT services to end users. The DOJ will continue delivering reliable services to maximize the use of cloud computing and modern applications, increasing productivity through new communication and collaboration tools, and developing strategic relationships with business partners to enable self-service processes through increased intelligence in workflows and automation across common, repetitive tasks.

This effort is a long-term, multiyear commitment to transform the Department's IT enterprise infrastructure and centralize commodity IT services. In order to accomplish the outcomes of DOJ's IT Strategy, 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.
- **JABS / CAS Technology Modernization:** Replacing legacy systems with a modern, cloud-hosted solution. The new system integrates services into a single, modernized system and eliminates the need for customers to invest individually.
- **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.

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

As stewards of taxpayer funds, 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.

iii. Cybersecurity – Protect Critical Mission Assets (Goal 3)

With the threats to DOJ increasing in frequency and complexity, protecting DOJ mission assets continues to be a top priority for DOJ leadership. To achieve the objectives of DOJ's IT Strategic Plan, 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, 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.

iv. Innovation Engineering - Build Innovative Capabilities (Goal 4)

As the DOJ mission advances, 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, 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, OCIO has initiated the development of a DOJ Artificial Intelligence (AI) Strategy to maximize mission support.

V. Program Increases by Item

Item Name: **SolarWinds Incident Response**

Budget Decision Unit(s): Justice Management Division (JMD)

Organizational Program: Justice Information Sharing Technology (JIST)
Program Increase: Positions: 0 Agt/Atty: 0 FTE: 0 Dollars: $78,786,000

Description of Item

The FY 2022 discretionary request identified a cyber reserve of $750.0 million. The FY 2022 President's Budget allocates these resources to nine agencies that were significantly impacted by the SolarWinds incident, one of which is the Department of Justice. The purpose of the funding is to address immediate response needs and does not focus on wholesale replacement of IT systems at this time. The funding request targets critical cybersecurity needs at these nine agencies which prioritizes basic cybersecurity enhancements, including: cloud security, Security Operations Center (SOC) enhancements, encryption, Multi-Factor Authentication (MFA), increased logging functions, and enhanced monitoring tools. Each agency's maturation levels were reviewed in these areas to determine the most critical gaps that require additional funding.

The FY 2022 President's Budget requests $78.8 million to address the impacts of the SolarWinds incident at the Department of Justice.

The SolarWinds supply chain attack, orchestrated by an advanced persistent threat actor, demonstrates the increasingly persistent and sophisticated cyber actors and campaigns threatening vital Federal Government networks. The Department is a key player in ensuring the integrity and operability of these mission critical IT systems supporting the American people. As such, a top priority of OCIO's Justice Security Operations Center (JSOC) is to prevent, detect, respond, and remediate the damage from malicious cyber attacks and espionage against the Department and Federal Government. Key enhancements will be made to modernize the Department's cybersecurity capabilities to support the JSOC mission.

- **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 and/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 will augment our logging capability to leverage cloud service provider Application Programming Interfaces to provide visibility into workloads, modifications, and enhanced response capabilities. In tandem, DOJ will

implement improved logging within the Department's cloud-based email system in order to enable better detections of adversarial access and activity. Additionally, DOJ will implement a baseline solution that monitors the health and management of network devices and systems.

- **Cloud Security Upgrades**

  DOJ will enhance its O365 licensing across all Department users in order to unlock additional security features such as advanced auditing of mailboxes and improved alerting of anomalous activity. These additional features 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.

- **Security Operations Center Maturation**

  The implementation of the cybersecurity initiatives to enhance JSOC monitoring and visibility will require an increase in support. In addition to the initiatives across logging, monitoring, and cloud visibility, the JSOC will implement deceptive technology, or honeypots, as a technique to secure high value assets and disrupt threat actor lateral movement by misleading or confusing the adversary through intentionally exposing decoy assets. Finally, the JSOC will plan and coordinate the implementation of zero-trust network capabilities to change the paradigm to enhance how DOJ applications are defended, accessed, and monitored.

- **Multi-Factor Authentication (PIV) / Encryption**

  The Department will also move to a centralized identity provider and authentication model, which will eliminate the individual federated component trust model exploited in the compromise, and create a universal, mandatory multi-factor authentication. Under this new model, trust will be established at the individual user and/or device level using OMB's mandated PIV as the strong, second form factor, which will also require DOJ to implement a secure certificate management system to effectively distribute and manage these authenticators. Additionally, leveraging the same authenticator, DOJ will implement user level encryption enhancing the ability to protect data while implementing the necessary capabilities for eDiscovery and records management.

Justification

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 security posture. Increasing the security of DOJ is a significant undertaking that requires a substantial investment in the requirements, architecture, design, and development of systems, system components, applications, and networks. OCIO will modernize endpoint detection and response, authentication, cloud security, audit logging, and the JSOC to

limit the impact and improve the detection and response to supply chain attacks. These investments will protect the DOJ enterprise by focusing on endpoints, data, and identity.

Impact on Performance

Risk management remains critical to the way DOJ protects its information, systems, and assets and improves its overall security posture. The Department will continue to refine this process by observing lessons learned and the evolution of the threat landscape. DOJ plans to integrate information gained from the SolarWinds event into broader IT modernization work, budget discussions, mission delivery activities, and security initiatives to reduce duplication and ensure alignment and prioritization of remediation activities across the Department.

1. Base Funding

FY 2020 Enacted				FY 2021 President's Budget				FY 2022 Current Services			
Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)	Pos	Agt/ Atty	FTE	Amount ($000)
0	0	0	$0	0	0	0	$0	0	0	0	$0

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2022 Request ($000)	Positions Requested	Full Year Modular Cost per Position ($000)	Annualizations ($000)			
				1st Year	2nd Year	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
N/A	$0	0	$0	$0	$0	$0	$0
Total Personnel	$0	0	$0	$0	$0	$0	$0

3. Non-Personnel Increase/Reduction Cost Summary

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Total Non-Personnel (Hardware, Software, Contractor Support)	$78,786	$78,786	1	0	0
Total Non-Personnel	**$78,786**	**$78,786**	**1**	**0**	**0**

4. Total Request for this Item

Category	Positions			Amount Requested ($000)			Annualizations ($000)	
	Count	Agt/ Atty	FTE	Personnel	Non-Personnel	Total	FY 2023 (net change from 2022)	FY 2024 (net change from 2023)
Current Services	0	0	0	$0	$0	$0	$0	$0
Increases	0	0	0	$0	$78,786	$78,786	$0	$0
Grand Total	**0**	**0**	**0**	**$0**	**$78,786**	**$78,786**	**$0**	**$0**

5. Affected Crosscuts

The Cybersecurity crosscut will be affected by this request.