U.S. Department of Justice Information Technology Strategic Plan

for Fiscal Years 2022-2024

U.S. Department of Justice
Office of the Chief Information Officer

Table of Contents

Message from the CIO

I am pleased to present the U.S. Department of Justice (DOJ or Department) Strategic Plan for Information Technology (IT) for Fiscal Years (FY) 2022–2024. The strategic plan reflects our vision over the next three years for DOJ to be at the forefront of delivering advanced systems and be a vehicle to address DOJ's critical mission challenges. Our vision includes the Office of the Chief Information Officer (OCIO) becoming a trusted provider in delivering exceptional services to meet the DOJ mission. We will continue to meet our customers' needs by providing reliable and efficient core offerings, while exceeding their expectations by adding new IT capabilities to execute the mission and improve operations in innovative ways.

Technology and information management are key enablers of DOJ's mission, from law enforcement, to the fair administration of justice, to public safety against foreign and domestic threats, to providing federal leadership on crime prevention and control. The boundaries of technology continue to be pushed, and it is imperative that our services enable the Department to effectively navigate the dynamic pace of technological change and data proliferation. Cyber-attacks are constantly challenging DOJ and other agencies. Therefore, we will continue to diligently protect the agency's critical data through increased cyber resilience and risk reduction while optimizing data utilization to create consumable and intelligent products.

In executing this IT Strategic Plan, the Department will work closely with the DOJ Components – our primary mission partners – to address the most pressing challenges facing the Department. In developing this plan, we included Component feedback to address their specific pain points. The goals and objectives set forth in this document will guide DOJ's use of technology to enhance security capabilities, leverage new technologies to meet customer needs, develop a strong and collaborative IT workforce, and improve financial stewardship of IT. We must identify opportunities for technology to improve processes, explore new capabilities, support workforce needs, and scale solutions to keep the Department at the forefront of technology, information management, and service delivery.

I would also like to thank the DOJ's IT professionals who will help drive the execution of this strategic plan. With their dedication and perseverance, we will make our information technology vision for DOJ into a reality.

Sincerely,

Melinda Rogers

Deputy Assistant Attorney General
Chief Information Officer (CIO)
Chief Data Officer (CDO)
Department of Justice

Executive Summary

The DOJ IT Strategic Plan for FY 2022–2024 describes our goals and objectives over the next three years to evolve our organization for the benefit of the DOJ mission, our workforce, and our partner organizations and stakeholders. Our focus in the strategy is mission enablement through technology. Our vision for the future of DOJ technology is aligned to the Department's priorities so that we are moving in lockstep with the overall enterprise plan. This includes the Department's strategic priorities on enhancing cybersecurity, achieving management excellence through innovation, leadership development, and furthering diversity, equity, inclusion, and accessibility to foster a talented workforce representative of the public we serve. Our vision is also aligned to priorities in the President's Management Agenda, the recent Executive Order on Improving the Nation's Cybersecurity, and the subsequent DOJ Deputy Attorney General Comprehensive Cyber Review.

Several factors played a major role in shaping the direction in which we will take DOJ technology and our subsequent strategic plan. They include:

User experience expectations

Increasingly sophisticated cyber threats that impact our mission

Growing technology complexity

Demand for distributed workforce operating models

Optimizing Resources

User Experience

As part of OCIO's continued adoption of ITIL principles, including the practice of continuous improvement, we must adapt to provide the high-quality services and speed to delivery that the mission requires. We recognize that successfully implementing technology for mission outcomes is driven not only by what technology is selected, but primarily by how it is developed and tailored to the unique mission needs of each customer. Over the past three years, we invested significant capital at DOJ on customer and user experience - how a user interacts with and experiences a product, system, or service - and we will continue to build on those efforts. A well-planned user experience provides a considerable return on investment to the Department by fulfilling customer needs, increasing productivity, collaboration, and engagement, optimizing development time and costs, and building a relationship of trust and partnership between IT and program offices.

Cyber Threats

Over the last decade we have seen a growing threat to government and commercial entities alike in the form of cyber attacks originating from a wide array of players: foreign intelligence services, criminal groups, hacktivists, and insider threats. The attacks have grown in sophistication, from exploiting systemic weaknesses in authentication architecture to ransomware attacks to social media misinformation to attacks on supply chains and industrial controls. These all pose significant danger to our nation's critical infrastructure and cost millions of dollars to government and commercial organizations to recover from attacks. Combating cybercrime and cyber-enabled threats to our nation's security remains among DOJ's highest priorities as part of our Department's mission to ensure public safety against threats foreign and domestic, and to provide federal leadership in preventing and controlling crime. These threats require us to fortify our existing technology environment and update our approach on how we advise other organizations on cyber capabilities. Our initial focus is to expand and reinforce a resilient enterprise that is both well-protected from threats and has the mechanisms to rapidly recover from attacks with minimal disruption to our mission operations. As we build our own capabilities, our experience will inform how we help the organizations we advise on cybersecurity to do the same.

Technology Complexity

Technology is rapidly changing how people work. Intelligent automation, robotic process automation, artificial intelligence, machine learning, and natural language processing, to name a few disciplines, all show great potential in transforming operations. In a rapidly evolving and increasingly more complex digital landscape, our goal is to become the technology advisor and implementation partner of choice to the mission areas. This is so that we can enhance mission operations and support the DOJ workforce in an impactful way while effectively managing the cost of risk with a more sophisticated technology environment. In addition to becoming savvy on emerging technologies, standardizing architecture and improving governance and oversight will be critical to manage costs and integrate different solutions into our technology ecosystem. We plan on being at the forefront of understanding and applying best practices to accelerate technology adoption and integration into the mission.

Distributed Workforce

The Department's success in operating a secure hybrid work environment during the COVID–19 pandemic illustrated the adaptability of our organization and people. We see the need for new and flexible tools, policies, and mindsets to support a distributed workforce more effectively and securely. While a distributed and remote workforce was a part of the DOJ operating model prior to the global pandemic, this capability has exponentially become a much larger part of our workforce operations. Effectively using technology will continue to enable the Department's people to be productive, communicate and collaborate well to execute mission responsibilities, and maintain our DOJ culture even while working remotely.

Optimization of Resources

As we tackle the factors listed above, we will continue to examine our operations for cost savings that could be used to support our strategic initiatives. We must accurately forecast the budgets and resources needed to execute our strategic priorities. To do so, we will need to set up practices to enable cost transparency that will support better planning and decision-making in allocating resources to our most important projects, initiatives, and assets.

Mission

Provide innovative, high-quality, and secure IT capabilities that support the Department in upholding law, justice, and public safety.

Vision

Deliver exceptional IT services and innovative capabilities, while transforming our workforce to continually adapt to a future of accelerating change.

Over the next three years, we will focus on improvements to better support DOJ staff and instill greater trust in our systems and services through achievement of the following goals:

1

Enhance Service Delivery

2

Elevate Cybersecurity

3

Embrace Innovation

4

Expand the Workforce

5

Increase Financial Transparency

This IT Strategic Plan will go in depth on the five goals, each of which includes specific objectives and initiatives. Taken together, these should not be viewed as sequential, but as interdependent with the collective purpose of providing the best possible IT services to our customers during a time of accelerating change.

Goals & Objectives

Goal 1: *Enhance Service Delivery*

Objective 1.1: Establish a customer-centric culture that delivers services that meet the dynamic and evolving needs of the Department's mission
Objective 1.2: Deliver industry-leading service management practices to improve reliability of IT services and vendor accountability
Objective 1.3: Use innovative new capabilities and service offerings to improve or enhance mission operations

Goal 2: *Elevate Cybersecurity*

Objective 2.1: Reinforce DOJ's cybersecurity foundation
Objective 2.2: Implement Zero Trust principles and tools to combat access-based threats and harden the defense of information systems
Objective 2.3: Enhance cloud security to support the Department's growing cloud adoption
Objective 2.4: Proactively manage IT supply chain risk across the DOJ enterprise throughout the IT lifecycle

Goal 3: *Embrace Innovation*

Objective 3.1: Create a culture of innovation to reduce barriers for adopting emerging technology
Objective 3.2: Optimize infrastructure and applications to enhance mission-critical operations and collaboration
Objective 3.3: Implement intelligent automation to enhance productivity and efficiency
Objective 3.4: Enhance data sharing and data governance standards to maximize value of information assets and enable collaboration

Goal 4: *Expand the Workforce*

Objective 4.1: Enhance recruitment and retention strategies to ensure staffing meets the demand
Objective 4.2: Upskill workforce to keep pace with the transformative impacts of emerging and expanding technologies
Objective 4.3: Enable the workforce to be agile and responsive so that DOJ can work efficiently without disruption

Goal 5: *Increase Financial Transparency*

Objective 5.1: Standardize financial management practices so that DOJ can gain greater insight into IT costs
Objective 5.2: Support strong governance of IT investments and acquisitions so that DOJ can realize the full value of technology for the entirety of its lifecycle

Goal 1: Enhance Service Delivery

We aspire to consistently provide an excellent customer experience and the tools to help mission staff increase their productivity. By delivering this experience through high-quality, customer-focused services, we will further enable our workforce to advance DOJ's law enforcement and litigation capabilities and grow confidence throughout the Department in reliable IT support and services. We will accomplish this by leveraging the voice of the customer, holding vendors accountable, and monitoring services to provide quick responses and achieve optimal service stability.

Objective 1.1 *Establish a customer-centric culture that delivers services that meet the dynamic and evolving needs of the Department's mission*

As technology is integrated in every aspect of the Department's mission and as customer experience becomes an increasing priority, we must develop a culture of service delivery that focuses on creating an optimal experience for both our internal and external customers.

Initiative 1.1.1: Leverage voice of the customer to continuously improve Department technology services delivered to the mission

DOJ will use voice of the customer to understand where services and customer engagement can be improved. A unified brand and communication plan will allow us to better engage with our customers to provide a common, high-quality, experience. To accomplish this, we will augment our practices related to communications, requirements gathering, validation, and retrospective activities. This will include determining targeted methods to obtain customer feedback so that gaps in service delivery are identified and remediated.

We need a customer centric culture to understand where services could be improved and how user experience could be enhanced to benefit our customers. We will increase the connection between OCIO service owners and customers by training both business process owners and service owners to understand the customer's perspective. This will allow them to verify our technology services are high quality and meet customer's needs. We will offer additional focused training for service owners to continually acquire industry best practices on customer relationship management, delivery excellence, product lifecycle management, and service ambassadorship. By consistently evaluating service delivery and incorporating best practices, our service offerings will constantly be improved to match industry standards and add business value.

Expected Benefit: DOJ IT services are able to meet customer needs as services evolve through our constant improvement of delivery and effective engagement with customers.

Objective 1.2 *Deliver industry-leading service management practices to improve reliability of IT services and vendor accountability*

We are responsible for ensuring that the services we contract from providers and the services offered to our customers are reliable, resilient, and transparent. Especially after large-scale cyber attacks, it is more important than ever that we closely monitor services to detect abnormalities. Building on our service management efforts and ISO 20000 certification, we will continue to work with our partners and customers to deliver high quality IT services.

Initiative 1.2.1: Increase service resiliency

Effective use of technology is critical to the Department's mission and requires limited disruption of service. To prevent unexpected or recurring failures of service, we must enhance our service management practices, such as performing post-incident analysis to apply lessons learned and enhancing configuration management to clearly define connections and dependencies across the environment. We will also prioritize using enhanced cloud technology features for disaster recovery to increase service resiliency and reliability. Resilient services will decrease downtime and allow DOJ services to remain operational when unexpected events or challenges arise.

Initiative 1.2.2: Enhance service monitoring

DOJ must closely and proactively monitor the services it offers to improve delivery of reliable service and detect abnormalities that could cause disruptions in service or result in a security breach. We will expand OCIO's new application monitoring offering to additional Components and enhance cloud asset monitoring (see initiative 2.3.1). Through increased visibility into the performance of services, we can minimize disruptions, verify that metrics meet or exceed performance standards, and ensure that any inconsistencies that are caught are responded to and remediated quickly.

Initiative 1.2.3: Enhance vendor accountability

As a consumer of commercial services such as cloud and eDiscovery products, DOJ works with vendors to ensure that services run smoothly and efficiently. We will establish enforceable Service Level Agreements (SLAs) for services that do not currently have one in place or ones that are not sufficiently robust. This will allow us to be a liaison for our customers and be able to hold vendors accountable to a comprehensive set of metrics, responsibilities, and expectations for both parties.

Expected Benefit: Industry best practices are implemented to increase dependability of services, minimize downtime, and improve visibility into costs and performance.

Objective 1.3 *Use innovative new capabilities and service offerings to improve or enhance mission operations*

In an evolving digital landscape, we need enhanced technological capabilities to fulfill mission activities. Powerful new technological tools now make it easier than ever to uncover insights and keep pace with the rapid expansion of digital information that is available to us. Enhancing services and capabilities will allow DOJ to better carry out law enforcement activities, deter threats, and hold bad actors accountable.

Initiative 1.3.1: Enhance tools or solutions that enable the Department's investigative and prosecutorial activities and back office functions

Our mission staff need enhanced technology capabilities to effectively carry out investigative and prosecutorial activities. We will partner with mission stakeholders to develop these capabilities. For example, JMD will will conduct an analysis of alternatives to implement a cutting-edge eDiscovery solution that will allow users to conduct discovery and identify evidence more efficiently. To enhance their grants management process, OJP will continue to build out the JustGrants system, which will implement a single grants management system for all three DOJ grant-making Components. JustGrants will offer streamlined end-to-end processes, to enable more funding and research that strengthens the justice system. JMD will continue to use innovative technology to support decision-making. For example, to address COVID attestation requirements, JMD created a dashboard using R statistical modeling tools to determine COVID trajectory for DOJ office locations.

Initiative 1.3.2: Advance law enforcement service offerings to better support the mission

State and local law enforcement require advanced service offerings to help support officers in the field. To enrich our service offerings, we will implement the Fix NICS system to enhance the database for firearms purchases. Through the implementation and management of technology, we will support the Deputy Attorney General's body-worn camera initiative to capture and enhance video and audio evidence collection. We will also strengthen our biometric capabilities as a service to deliver a modernized and integrated solution to law enforcement officers across the United States. These enhancements will allow state and local law enforcement to conduct criminal justice activities in a more accurate and lawful way that aligns with the DOJ mission. To enhance the mobility of staff and embrace innovative technology, BOP is upgrading wireless technology throughout their Inmate Housing Units. This technology will improve medication dispensing, enhance security to detect unauthorized mobile devices, and support staff in monitoring and tracking activity in the units.

Initiative 1.3.3: Support modernization of Records and Information Management

DOJ is undergoing an effort to modernize its records and information management program and tools. To help achieve the goals and objectives of this initiative, DOJ IT will support enterprise tools to address gaps in current technology. The Department is assessing new technology to offer to all Components as part of a shared service model to address common requirements and business needs. Over the next year, we will also create an information management strategy, and enhance governance to better manage data, information, files, and knowledge. These efforts will help DOJ better respond to changing Federal requirements and regulations related to managing records and information, increase efficiency and effectiveness, reduce risk across the organization, and better meet mission needs.

Expected Benefit: DOJ will develop new services and enhance existing ones in a timely manner to continuously improve our mission operation capabilities.

Goal 2: Elevate Cybersecurity

DOJ must be a standard of excellence for cybersecurity to effectively support our mission and our many stakeholders who rely on us for security capabilities. We must lead and drive our cybersecurity and identity practices to address challenges within the Department. These challenges include vulnerabilities introduced by the increased use of remote access and our current identity and access management (IAM) configuration. The outcome we seek is to strengthen our security posture against complex cybersecurity attacks, improve and fortify internal remote access for our mobile workforce, and streamline our identity and access management.

Objective 2.1 *Reinforce DOJ's cybersecurity foundation*

Initiative 2.1.1: Enhance asset inventory management

DOJ will continue to strengthen its asset management processes and tools, as well as use automation techniques to inventory and track assets. We will continue to use a rigorous and systematic process to deploy end-point management agents to all assets in the DOJ environment. All assets will be scanned and managed, as this is a critical safeguard to protect DOJ from cyber attacks and enhance our awareness of potential risks. To better manage assets, we will enforce the persistent deployment and management of Endpoint Lifecycle Management System (ELMS) agents to every laptop, desktop, and server, as well as scan for devices such as routers and switches. DOJ will make a concerted effort to identify any unmanaged devices and bring these under the asset management process.

To better secure devices, DOJ will be moving away from traditional deny listing, and implementing an allow listing approach. Allow listing will permit DOJ to scan applications before they are added to devices.

Initiative 2.1.2: Modernize monitoring and management of internet traffic

DOJ will continue to support the foundational principles of its traditional Trusted Internet Connection (TIC). While maintaining the TIC to preserve our foundational tools, DOJ is adopting a Zero Trust architecture (ZTA) to evolve the DOJ's cybersecurity program. Although our traditional TIC scope and purpose will be reduced through ZTA, the TIC will still support our on-premise technology, in-bound traffic for public-facing systems, and our operations as we transition to the full ZTA model.

Initiative 2.1.3: Focus on cyber hygiene to reduce risks to DOJ

DOJ must ensure its management of vulnerabilities are compliant with new Federal mandates related to risk reduction, through reducing and managing risk of legacy Plans of Action and Milestone (POA&M) and end-of-life software. The Enterprise Lifecycle Management System (ELMS) will provide an enhanced review of all software and allow inventory of what is at end-of-life and transition these assets off the network. We will work with Components to proactively manage end of life software using ELMS information. The OCIO team will work with Component System Owners to implement this review and remediation process.

DOJ will increase its capabilities in vulnerability management. We have implemented a Vulnerability Disclosure Program (VDP) based on new OMB requirements. This program allows the public to report vulnerabilities related to DOJ's public-facing applications and systems. We will support system owners with tracking and remediating these vulnerabilities to better protect our critical assets. We will also focus more heavily on the continuous assessment of public-facing applications and systems for exploitable vulnerabilities. DOJ will also focus on enhancing its penetration testing capabilities by conducting ground truth testing for all systems. Ground truth testing will help DOJ reduce risk and mitigate vulnerabilities.

Expected Benefit: DOJ uses its strong foundation of tools and capabilities to manage threats and reduce risk for the organization.

Objective 2.2 *Implement Zero Trust principles and tools to combat access-based threats and harden the defense of information systems*

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, DOJ must modernize its approach to cybersecurity. Large-scale security breaches and supply chain attacks from foreign nation states highlight the need to accelerate cyber security efforts such as transitioning to ZTA. ZTA is a holistic approach to cyber security that is rooted in the principle of never trust, always verify. It removes the concept of implicit trust and instead requires a contextual approach that includes the application, user, and device to allow for access decisions to adjust based on the context of the user.

To address these threats over the next three years, DOJ will focus on identity management including use cases between DOJ and external, non-federal entities, implementing a Zero Trust Broker, and utilizing automated Endpoint Detection and Response.

As part of integrating ZTA, DOJ must address its current authentication architecture with over 20 Identify Providers (IdPs) by centralizing to one IdP. The use of multiple IdPs results in several challenges: (1) without consistent cyber practices and standards, certain IdPs may be more vulnerable to remote access cyber attacks, and (2) multiple IdPs cause an administrative burden for staff across Components to collaborate on information residing across the Department. Integrating ZTA and centralizing identity will not only improve our security posture against threats but also internally improve mission collaboration through enhanced access to systems and data across Component boundaries.

Initiative 2.2.1: Unify identity and access management across the Department

Our current IAM configuration needs to be modified to centralize authentication. We will simplify our current architecture for authentication by combining the Department's Identity Providers into one, unified Identity Provider. As part of our process to centralize our IdPs, we will require users to authenticate using a Personal Identity Verification (PIV) credential, with strong credential issuance and non-PIV multifactor authentication temporarily permitted only for non-PIV edge cases. A centralized source of identity will improve our ability to govern and automate access control with attributes and prohibit bad actors from impersonating DOJ personnel.

Initiative 2.2.2: Mitigate internal and external access-based threats while improving user experience

A ZTA strengthens our robust security posture and enables DOJ to secure, manage, and monitor every device, user, application, and network transaction occurring throughout the network. We will transition to ZTA to utilize identities, attributes, dynamic access policies, and strong credentials. The implementation of ZTA will not only address internal and external access-based threats but will also create a streamlined and frictionless user experience for DOJ employees. The transition process includes implementing a Zero Trust Broker to facilitate the removal of Virtual Private Networks (VPNs) from the DOJ network, improving the workforce's ability to be mobile. ZTA normalizes access and performance across all resources regardless of the location of the technology (e.g., cloud, data center) or staff (e.g., remote, onsite).

Implementing a modern approach to cybersecurity like ZTA will also require new governance and guidelines for Department-wide coordination. OCIO will take the lead on implementing a ZTA governance structure to ensure collaboration with Component IT offices. We will use our existing Departmental CIO Council Cybersecurity Committee, an integrated DOJ-wide cybersecurity governance structure, to track Department- wide progress for ZTA implementation. Successfully utilizing ZTA will improve mission collaboration through improved access to systems and data across Component boundaries and simpler user experience.

While implementing ZTA, DOJ will coordinate the transition off legacy networks to Internet Protocol version 6 (IPv6). IPv6 has feature and performance benefits required in today's interconnected world. Modern network innovation and standards are occurring in IPv6, and as a result, major networks and content providers are migrating to IPv6–only infrastructure.

Initiative 2.2.3: Strengthen threat detection, response, and remediation

To provide greater protection against a broad range of threat actor tactics and techniques, the Department will expand Endpoint Security to enhance the detection and blocking of advanced threats as well as incident response capabilities by installing Endpoint Detection and Response (EDR) agents on DOJ assets. EDR agents are also a key component of integrating ZTA as they provide device status to the Zero Trust Broker and DOJ's security operations center (SOC) for access decisions. This will support DOJ in understanding the security posture of our assets and provide enhanced visibility into our endpoints, regardless of their physical location.

Expected Benefit: DOJ will use ZTA to holistically transform the security paradigm and reduce access risks, while supporting a seamless user experience. DOJ will be better equipped to deter and protect against cyber attacks and remediate any damage caused by potential breaches in a timely manner.

Objective 2.3 *Enhance cloud security to support the Department's growing cloud adoption*

As DOJ continues to use cloud technology, we need do so in a coordinated, deliberate way that allows us to prevent, detect, assess, and remediate cyber incidents. In order to protect cloud data from threats, the Department will need to closely monitor and manage cloud accounts and services while also integrating new technology to increase security. We will focus on three key areas, including improving our cloud service management, enhancing cloud monitoring, and better securing cloud access.

Initiative 2.3.1: Centralize cloud monitoring and secure access to cloud services

The Department will continue to move assets to the cloud and enhance our cloud inventory of systems and service information (e.g., account and subscription IDs), which will allow the Department to track our cloud use and avoid costs like redundant accounts.

We will centralize and streamline cloud monitoring to drive analytics for identifying and managing cybersecurity risks to DOJ's High Value Assets (HVAs). To accomplish this, we will centralize auditing and Justice Security Operations Center (JSOC) monitoring of cloud administration activities to closely track security and performance data. This includes integrating cloud administration activity into the JSOC for 24x7x365 monitoring, alerting, and incident response, starting with enterprise cloud applications and Infrastructure as a Service (IaaS) environments. We will also implement a Security Posture Dashboard (SPDR) for the network to allow DOJ to gain insight into all cloud assets and understand the health of the network. Cloud monitoring increases visibility into our cloud computing environment and positions the Department to better detect potential threats and manage performance.

Expected Benefit: DOJ can continue growing cloud use in a secure and responsible way.

Objective 2.4 *Proactively manage IT supply chain risk across the DOJ enterprise throughout the IT lifecycle*

DOJ will strengthen its IT supply chain management practices by incorporating risk management principles and activities related to cybersecurity into existing processes. This will allow DOJ to proactively identify vulnerabilities that may exist, helping to prevent cyber attacks and breaches and reduce overall risk to the organization by better managing our critical assets.

Initiative 2.4.1: Identify the IT supply chains that support DOJ's mission-essential and critical services

To understand where there may be risk in DOJ's supply chain, DOJ must first have a thorough, comprehensive, and continuous understanding of its vendors and the software and hardware being used across the Department. For systems that are operational today, DOJ will document the most mission-critical supply chains, identifying vendors who support DOJ's mission-essential systems.

These efforts will help DOJ comply with the Federal government-wide initiative to require a Software Bill of Materials (SBOM). The objectives of the SBOM are to understand what components are used in software that is purchased from vendors, to collectively monitor and discover any potential vulnerabilities in the software, and to determine what systems may be impacted to mitigate risk. Over the next three years, DOJ will work diligently to incorporate new processes into our IT lifecycle and vendor management to better manage potential risk in software purchased from vendors. This process will improve our understanding of our purchased software inventory and how we manage it.

Initiative 2.4.2: Develop an enterprise-wide view to monitor IT supply chain risk across DOJ

After DOJ has inventoried the vendors and software that impact mission-critical systems, we will use this information to develop an enterprise-wide view of the IT supply chain and risk associated with it. DOJ will create processes and tools to conduct this effort, leveraging existing tools like SPDR and creating new ones, where needed. These tools will help DOJ see where there is risk in the supply chain by identifying what Components are using certain vendors, what risk scores exist for vendors, what components of systems may be or are impacted by vulnerabilities, and where actions need to be taken to address vulnerabilities or risk. We will use this information to reduce and manage risk in DOJ's portfolio to protect our assets and environment.

To better manage the IT supply chain, DOJ OCIO will leverage its IT Investment and Acquisition Review (ITAR) process. We will modify existing ITAR processes to ensure we can identify IT procurements with elevated supply chain risk early in the acquisition process. DOJ needs better transparency and a centralized view into IT acquisitions and supply chain risk associated with these purchases. This will better equip DOJ to respond to new NIST and OMB guidance and regulation to execute supply chain controls over the next three years. DOJ OCIO will work with Component System Owners and Authorizing Officials to implement new controls related to supply chain.

Expected Benefit: By proactively managing the IT supply chain, DOJ will be able to better identify vulnerabilities that may exist, prevent cyber attacks and breaches, and reduce overall risk to the organization.

Goal 3: Embrace Innovation

By supporting information sharing and collaboration across DOJ and removing barriers to technology adoption, we will accelerate innovation. As a result, DOJ will be better able to use data to make strategic decisions, modernize IT systems, and capitalize on new technologies that help us complete litigation and law enforcement activities more quickly and efficiently.

Objective 3.1 *Create a culture of innovation to reduce barriers for adopting emerging technology*

The environment we operate in requires us to adapt actively and continuously. To remain at the forefront of technological change, DOJ must have the infrastructure and resources to aid exploration and pursuit of emerging technology.

Initiative 3.1.1. Foster collaboration and technology adoption through Communities of Interest and engineering groups to drive innovation

Communities of Interest (COIs) have proven to be useful tools for uniting staff throughout DOJ to accelerate adoption of new technologies and practices. We will continue to improve the use of COIs as a forum for sharing best practices on emerging technology and coordinating on department-wide initiatives. We will also continue partnering with other federal agencies, private industry, and academia to create channels for knowledge sharing with the COIs. We will expand the innovation engineering group efforts to prototype solutions and introduce them to Components and partners. We will develop a lifecycle for innovation work that includes the effective introduction of new technologies and practices to DOJ.

Initiative 3.1.2. Create opportunities that allow for exploration and experimentation with technology products and practices

Organizations accelerate innovation via targeted exploration to determine which technologies could add value. Therefore, we will establish dedicated infrastructure and supporting resources for a joint innovation
lab to accommodate department stakeholders and partners in the exploration and exhibition of emerging technology. This will accelerate the use of new capabilities and technologies throughout DOJ and among stakeholders to support the mission.

Expected Benefit: DOJ will accelerate innovation and adoption or scaling of emerging technologies that provide value.

Objective 3.2 *Optimize infrastructure and applications to enhance mission-critical operations and collaboration*

Mission-critical applications and capabilities must be able to meet the evolving challenges DOJ faces. As such, we require a modern IT infrastructure that is fully capable of supporting the mission and highly resilient to maintain mission operations.

Initiative 3.2.1: Expand adoption of cloud-based technology and conduct modernization of mission-critical applications to ensure the most effective software and hardware portfolio across DOJ

As good stewards of our IT investments we will continue modernizing major systems including eDiscovery and electronic records management. For example, BOP is planning on migrating SENTRY, BOP's inmate management system, to an AWS cloud environment. This will result in a lower total cost of ownership, a more efficient user experience, an enhanced ability to rapidly respond to new business needs, and better interfaces with DOJ's law enforcement partners.

BOP is also planning network infrastructure upgrades of the Local Area Network (LAN) to increase the bandwidth. The increased bandwidth of the LAN will permit the BOP to embrace innovative technology to support 25,000 new IP cameras at high quality resolution to address audit findings and increase the BOP's video conferencing capabilities.

Similarly, ATF will implement a contractor owned/contractor operated National managed LAN environment eliminating the need for capital purchases and government managed deployment. In so doing, ATF will be more agile when new technologies are deployed.

DOJ will mature the Core Enterprise Facilities (CEF) Hosting service per ISO processes and requirements and close non-CEF data centers. We will also continue to implement the Cloud Smart Policy along with an enterprise cloud policy, technology standards, and administer procurement vehicles for cloud. As components like BOP move to the cloud, they are practicing application rationalization processes by assessing the need for and usage of applications; and discarding obsolete, redundant, or overly resource-intensive applications. Decreased application management responsibilities will free agencies to focus on improving service delivery by optimizing their remaining applications.

Expected Benefit: DOJ's infrastructure and applications will effectively and efficiently provide the capabilities necessary to achieve the mission as the challenges we face change and evolve. This will allow us to take advantage of the benefits of cloud while ensuring that DOJ has the most efficient and effective hybrid and collocated IT infrastructure.

Objective 3.3 *Implement intelligent automation to enhance productivity and efficiency*

Intelligent automation such as Artificial Intelligence (AI) and Robotic Process Automation (RPA) offer the Department opportunities to enhance the way we work and accomplish our mission more efficiently and accurately than manual labor alternatives. AI can be used at the Department to quickly redact sensitive items within audio, video, and image-based evidence, and enable eDiscovery teams to transcribe, translate and perform object detection on large amounts of data across audio, video, and text-based files. RPA is being used across the Department to reduce process times for repetitive and highly manual tasks such as reviewing failed logon attempts and monitoring server failures saving our teams hundreds of hours of work annually. As we take advantage of these new technologies, we must also recognize the public safety implications of new technologies. Our efforts to implement intelligent automation rely on our ability to enhance our workforce and skills, collaborate on application of use cases, and define policies and guidance to reduce risk. We will follow the guidelines detailed in the Department's AI Strategy and Data Strategy, while complying with the Department's ongoing evaluation of the impact on civil rights and civil liberties by emerging and disruptive technology.

Initiative 3.3.1: Support use case development and adoption of ethical artificial intelligence and other automation practices and tools

To ensure DOJ adopts ethical AI practices based on existing statute, policy, our mission, plus civil rights considerations, and to comply with Executive Order 13960 Promoting the *Use of Trustworthy Artificial Intelligence in the Federal Government*, we will compile, annually review, and update an AI Use Case inventory. We will also continue to identify manual and time-intensive processes (e.g., financial management, records management, cybersecurity reporting and monitoring, and service delivery monitoring) to determine use cases and objectives for automation and AI-augmentation.

To ensure we equip the workforce with technical guidelines and decision aids for AI and RPA and other new technologies, the Artificial Intelligence COI and the Innovation Engineering group will lead the identification of use cases for intelligent automation and artificial intelligence. They will also pursue automation technologies or practices that will enhance operations and champion their implementation. To facilitate this, DOJ will create a test bed for AI that is cost sustainable and can be used across DOJ to safely explore and experiment. To expand their use of automation and equip their teams with the resources they need to implement new tools, ATF rewrote IT governance and change control processes to specifically support automation and continuous deployments. ATF will continue expanding cloud automation and DevSecOps practices across remaining systems and formalizing new governance policies.

Expected Benefit: DOJ will be better able to integrate automation that will maximize efficiency via computer-assisted processes that augment productivity and decision-making.

Objective 3.4 *Enhance data sharing and data governance standards to maximize value of information assets and enable collaboration*

We are improving the way the Department tracks the data we possess, who is using the data, what the data are being used for, and how the data should be protected. DOJ has been implementing a governance structure to standardize how Components analyze, send, and receive data across DOJ. We will continue to standardize governance to bridge gaps in data sharing and enhance our ability to get the most value out of our data.

Initiative 3.4.1: Continue to improve data governance, sharing, and collaboration to build a strong foundation for data analytics

To ensure that the data inventory is complete, accurate, and appropriate, we will continue to proactively and continuously communicate the purpose and value of the data inventory to all of DOJ, expanding the inventory with key attributes. We will also adopt a process for metadata management and data lifecycle management through the Data Strategy efforts. The management and organization of data assets to successfully utilize analytics will drive informed decisions in mission areas such as litigation and law enforcement.

To establish Department-wide guidance and best practices for data governance and data sharing, DOJ will identify and publish data exchange standards and practices, including inventory and risk assessment guidelines for data exchange with support from the Data Governance Board (DGB). We will also develop a data exchange framework for Components to document, control, and standardize how information is exchanged. An inventory of data exchanges will be retained within DOJ's data inventory. Through the implementation of DOJ Data Strategy and Geospatial Data Strategy, we will continue to increase compliance with open data requirements and reduce barriers for the public to access and analyze data. We will utilize public engagement for our priority datasets and increase value by hosting challenges.

Expected Benefit: DOJ will securely and efficiently share, access, and utilize data critical for mission activities (such as investigation and intelligence) across DOJ and with broader government and public.

Goal 4: Expand the Workforce

By maintaining a diverse workforce that has the skills and technology required to excel in their roles, DOJ will advance the mission with an agile, well-trained workforce that is empowered to adapt to the unexpected, deliver new technologies, and perform well from any location.

Objective 4.1 *Enhance recruitment and retention strategies to ensure staffing meets the demand*

We are going to invest in strategic recruitment and retention approaches over the next three years to grow and retain a diverse IT workforce of tomorrow. The Department currently has several vacancies for IT positions and our staffing level is below the desired threshold. Several factors contribute to this challenge, notably difficulty finding candidates with the skillsets required in addition to challenges retaining IT professionals. To address this, we are committed to partnering with Human Resources and other areas of the Department to attract, develop, and retain the IT workforce required for the Department to be successful.

Initiative 4.1.1: Partner with OHR to recruit a talented and diverse workforce

Attracting a strong workforce that has the skills the Department needs is critical to advance the DOJ mission. We will work with Human Resources to create and maintain a current position description library to aid in recruitment and clearly highlight the benefits of each position such as mission impact, work life balance, stability, a diverse and inclusive environment, and benefits unique to the public sector. We will also coordinate with Human Resources to analyze the recruiting process and determine ways to ensure the pipeline reflects our nation by being diverse, equitable, inclusive, and accessible while also having the skillsets needed to support DOJ, such as expertise in cyber and cloud.

Initiative 4.1.2: Enhance retention activities to maintain a strong workforce

For DOJ to be a model employer, with high employee engagement, we must invest in our employee experience. We will seek feedback to understand current employee sentiment and take action to address opportunities for improvement. We will also work with Human Resources to better define the career model for IT positions that lay out a clear path to help IT professionals grow their career. This will increase transparency of position expectations and provide greater clarity on career paths. We will also socialize our current benefits so that employees are aware that they can capitalize on programs like DOJ's student loan assistance, and institute incentives, where possible, like a cyber retention bonus.

Expected Benefit: We plan to rapidly fill vacancies and increase staff retention to help achieve a steady-state staffing level of greater than 90% so that OCIO staffing is sufficient to meet OCIO workload demand.

Objective 4.2 *Upskill workforce to keep pace with the transformative impacts of emerging and expanding technologies*

In order to apply emerging technologies to DOJ mission operations, we require a workforce with skills to use them. We are committed to making the investments to continue building a talented and diverse workforce with skills to build these capabilities. We will help our IT project and service managers grow their competencies in managing projects and financials, which will improve the consistency in managing IT project budgets. This will be critical for developing the workforce and building the capabilities DOJ needs.

Initiative 4.2.1: Establish opportunities to increase skills related to emerging technologies, cybersecurity, and business foundations

We must ensure the skill sets, training, certifications, and resources we need to develop our workforce capabilities are clearly defined and current. We will work to provide opportunities to all of DOJ through cooperative effort. As an example, we will partner with FBI and Huntsville Analytics to create a Data Science Academy, which will contribute significantly to our data and analytics efforts.

Our IT project and service managers come from a diverse array of professional experiences. To enable effective IT operations and consistently follow best practices in project management, agile methodologies (i.e., Scrum, Scaled Agile Framework [SAFe]), financial management, and vendor management, we will invest in building and maintaining competency throughout our manager population across key capabilities. We will assist our key leadership and managers in embracing the disruptive, yet proven techniques and technologies with industry recognized frameworks and coaching services. We will also provide training on financial management, forecasting, service planning, business planning, and service estimating so that our managers have a uniform understanding of delivering IT projects within budget.

Expected Benefit: An operational IT workforce that has the skills and capabilities to enable a secure cybersecurity posture and take advantage of emerging technologies to advance the Department's mission.

Objective 4.3 *Enable the workforce to be agile and responsive so that DOJ can work efficiently without disruption*

Being a model employer also includes evolving our workplaces and work practices to reflect the needs of our workforce today and tomorrow. With the increased adoption of a remote and potentially geographically distributed workforce, OCIO has provided the infrastructure and tools to support collaboration of staff working in a hybrid environment. DOJ will continue utilizing expanded flexibilities in work arrangements, such as expanded telework and alternative work schedules, and increased adoption of technology, such as cloud computing, collaboration tools, and automation. The workforce of tomorrow is supported by DOJ to work from anywhere at any time, securely and consistently.

Initiative 4.3.1: Ensure the workforce can work from anywhere at anytime

In addition to supporting an increasingly mobile workforce, DOJ must also accommodate the new status quo for hybrid working. To do this, we will enhance telework tools or introduce new ones, such as Virtual Desktop Infrastructure, to allow access from non-GFE devices and strengthen the security of our remote access solutions. As part of this shift to hybrid working, OJP will be moving to a new headquarters facility and will be implementing modernized technology to support the workplace of the future in support of both telework and onsite work.

To ensure our mobile workforce can effectively collaborate and remain productive at any work location, we will also enhance digital communication and collaboration capabilities with improved integration and full interoperability throughout DOJ. DOJ has made great strides towards this such as implementing Microsoft Office365 Department-wide and will continue to support the migration for Components like BOP who are moving 39,000 staff and 17,000 shared mail boxes to Office365. Office365 allows DOJ to build the IT workforce of tomorrow with the modern collaboration tools that can be accessed securely from almost anywhere. Beyond the technical and operational support for DOJ staff, we will ensure that policy is revised as needed to support workforce flexibility and productivity.

Expected Benefit: An IT workforce that can continue working with a high degree of productivity and collaboration to seamlessly continue to execute the mission.

Goal 5: Increase Financial Transparency

Strong IT financial management and investment tracking will help DOJ realize greater value from technology investments, gain insight into cost optimization opportunities, support contract oversight, and ensure that our IT capabilities are cost-efficient and driving benefits. We will implement standards and governance that improve our financial stewardship and enhance the way we manage our IT projects and acquisitions.

Objective 5.1 *Standardize financial management practices so that DOJ can gain greater insight into IT costs*

We must have clear visibility into total cost of ownership for IT projects and services. Since transitioning to the Department's Unified Financial Management System (UFMS), we must implement mechanisms to accurately track and report IT spending.

Initiative 5.1.1. Increase transparency into how DOJ is spending money on IT investments

To better manage and standardize financial management, and to comply with statutes and policy, a common platform for all Components is ideal. For DOJ the platform is UFMS; therefore, we will refine governance, policies, and standards to help Components onboard and use UFMS. This will allow DOJ to move towards a more structured and disciplined approach to financial management that adheres to a standard process. For example, we are leveraging UFMS by customizing processes within the system to better support our customers and improve our execution and reporting capabilities.

DOJ will follow a uniform taxonomy, and implement tools to standardize configuration of costs within UFMS and improve visibility into IT spending. This includes the development of the OCIO Billing Dashboard, where customers can view consumption metrics in real- time. The data provides customers actuals and projections against each consumption-based Reimbursable Agreement (RA), which enables our customers to make informed budgeting and planning decisions. The dashboard's metrics are also used as the basis for billing and will reduce the amount of coordination required between budget and finance counterparts. We will also integrate cloud cost management tools into IT cost models to help track cloud spend, forecast future cloud growth, and discover any cost inefficiencies. This will improve IT cost transparency and ensure the alignment of IT investments to strategic goals.

Expected Benefit: DOJ's financial management practices are enhanced to increase our understanding of IT expenditures and enable our ability to use data for informed decision-making.

Objective 5.2 *Support strong governance of IT investments and acquisitions so that DOJ can realize the full value of technology for the entirety of its lifecycle*

Smart technology investments help position DOJ for future growth and resilience. We can continue to make smart and efficient IT investments by leveraging data from similar procurements of IT products and services. Taking advantage of shared services where possible, will also allow us to avoid capability redundancies and help drive informed decisions when evaluating new technologies.

Initiative 5.2.1: Use prior cost performance and relevant technical requirements to enable data-driven decisions for IT acquisitions and engage appropriate stakeholders in the process

The implementation of standardized financial management practices will provide IT cost transparency and insight into the historical spend of IT projects and services. This will ultimately inform IT budget planning with assured, data-driven decisions. Components like OJP have been focused on optimizing the integrated review of IT solutions for investment that include business investment priority, engineering review, and project review equities of priority IT solutions that support program office mission and enterprise IT needs.

Initiative 5.2.2: Encourage use of shared services through key modernization initiatives

Promoting the reusability of products and acquisition vehicles as groups of capabilities or service functions that can be used across mission areas has allowed the Department to get the best value out of existing products. This includes collaborating with customers to identify needs and determine if there are existing tools or applications that can be used as a shared service. DOJ will be able to scale evolving IT, business, and mission needs while also providing streamlined allocation of IT investments.

Expected Benefit: DOJ can make smarter investments in technology that allow the Department to meet the needs of the mission more efficiently.

Appendix

The U.S. Department of Justice Information Technology Strategic Plan for Fiscal Years 2022–2024 is aligned with the strategic plans listed below.

DOJ Strategic Plan for Fiscal Years 2018 – 2022	**1**
DOJ Data Strategy	**2**
DOJ Geospatial Strategy	**3**
DOJ AI Strategy	**4**
DOJ IT Strategic Plan for Fiscal years 2019 – 2021	**5**

This document fulfills requirements listed in Circular A–130. The IT Strategic Plan is also Information Resources Management (IRM) Strategic Plan, as defined in the OPEN Government Data Act, Title II of the Foundations for Evidence-based Policymaking Act. (superseding the IRM SP defined in M–13–13) ***https://www.congress.gov/bill/115th-congress/house-bill/4174/text/enr#H6EB09243B14049C4B85D5A3C0A59E446***

Although this document covers fiscal years 2022 through 2024, there will be annual updates also to comply with OPEN Gov Data Act ***https://www.congress.gov/bill/115th-congress/house-bill/4174/text/enr#H4A4E1C65534449AE9649F09A1D55A12D*** *and the other guidance which may also require annual updates. These annual updates will be made available online.*