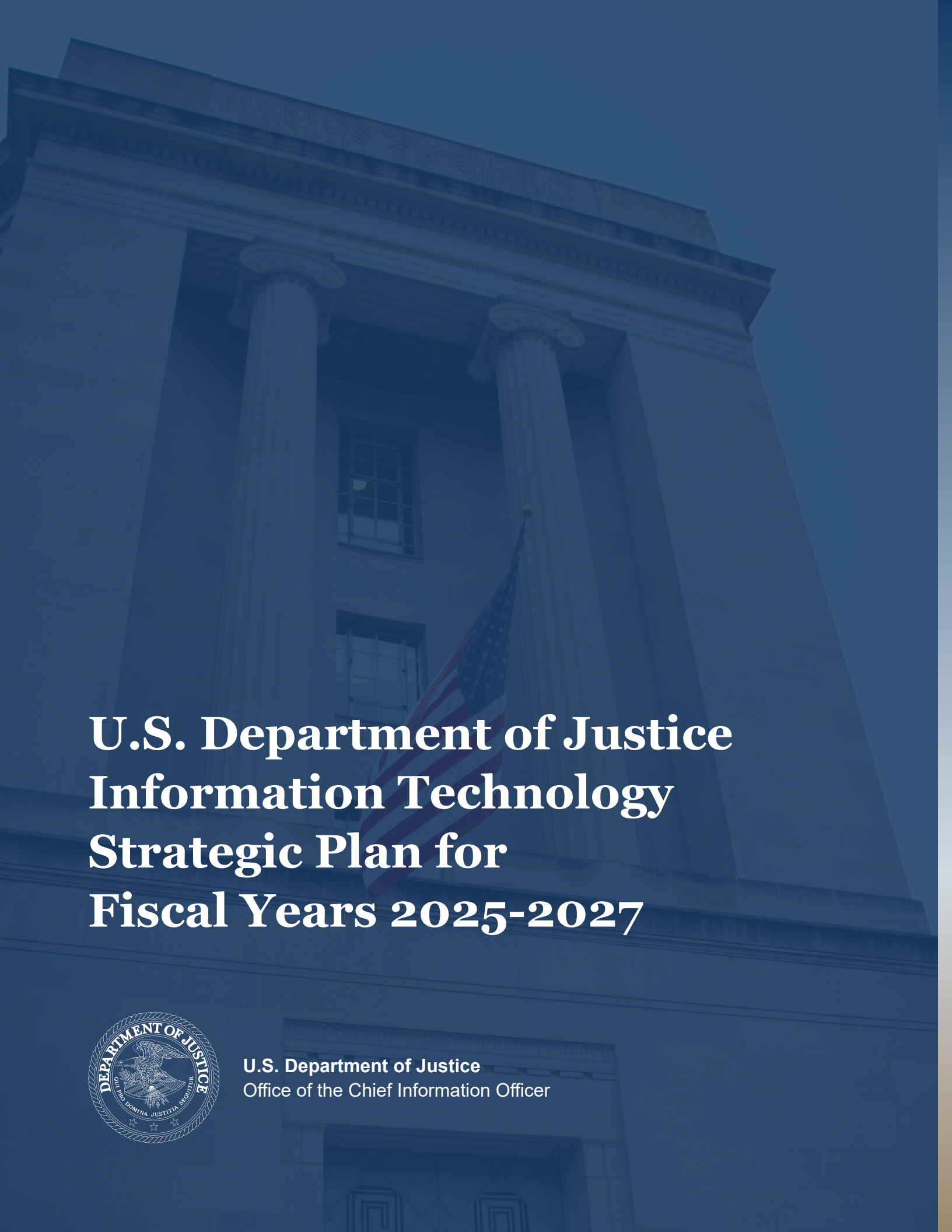


U.S. Department of Justice Information Technology Strategic Plan for Fiscal Years 2025-2027

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) 2025-2027. This strategic plan reflects our vision over the next three years on how the business of information technology would serve as a conduit to address DOJ's critical mission challenges, 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.

Our collective dependency on IT for daily activities, from the simple to the complex, continues to accelerate. An interconnected view of the entire Department and how the various components of our law enforcement, prosecution, and incarceration missions are supported by IT is critical for coordinating programs, managing priorities, and providing effective technology support to multiple transformation efforts. Increasingly, IT and cybersecurity professionals have become the indispensable, front-line warriors of this phenomenon, leveraging digital solutions to drive transformation, keep pace with innovation and provide resilient tools. Our customers expect and deserve excellence in delivery of IT services due to the essential nature of our support.

In executing the DOJ IT Strategic Plan, OCIO will collaborate with the DOJ Components – our primary mission partners – to focus on the Department's most pressing challenges. In creating this plan, we reviewed Component priorities and incorporated their feedback to refine the initiatives. The Goals and Objectives set forth in this plan will direct DOJ's use of IT resources to deliver mission-enabling services, augment cybersecurity capabilities, leverage new technologies to meet customer needs, build a skilled, collaborative IT workforce, and enhance financial stewardship of IT investments. In addition, we must optimize our core processes and develop scalable solutions to navigate the dynamic pace of technological change and data proliferation.

Lastly, I would like to thank the DOJ's IT professionals from across the organization for their contribution to the development of this strategic plan, and of course their implementation support to help us realize our vision.

Sincerely,

Melinda Rogers

Melinda Rogers
Deputy Assistant Attorney General
Chief Information Officer (CIO)
Chief Data Officer (CDO)
U.S. Department of Justice

Executive Summary

The DOJ IT Strategic Plan for FY 2025-2027 describes our Goals and Objectives over the next three years to enhance our support of the DOJ mission, workforce, and partner organizations and stakeholders. Our strategic focus is mission enablement through strong technology capabilities. 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, developing leadership, enabling data-driven decision-making, and fostering a talented workforce representative of the public we serve. In addition, the DOJ IT Strategic Plan supports priorities in the President's Management Agenda, Executive Orders, and other Federal mandates and policies.

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 mission-enabling digital solutions that adapt to the future of the organization.

Over the next three years, we will continuously enhance support of DOJ staff and optimize trust in our systems and services through achievement of the goals listed below. Taken together, these goals have the collective purpose of providing the best possible IT services during a time of accelerating change. For each of these five goals, the DOJ IT Strategic Plan includes specific objectives and initiatives.

Goal 1: Enhance Service Delivery

DOJ is committed to enhancing service delivery by leveraging modern tools like AI, cloud platforms, and streamlined workflows to improve efficiency, resiliency, and customer satisfaction. By prioritizing our digital operations, scalable applications, and accountability in our partnerships, the Department will increase its adaptability to risks, accelerate IT development, and ensure our stakeholders receive reliable and consistent support.

Goal 2: Elevate Cybersecurity

DOJ must uphold a standard of excellence in cybersecurity to address evolving challenges such as cloud technology vulnerabilities, IT supply chain risks, and advanced cyber threats. To meet these demands, we need to enhance our security measures by adopting advanced phishing resistant tools and furthering our Zero Trust practices. Strengthening identity ecosystems with advanced technologies, governance, and user-friendly solutions will ensure robust protection while supporting our stakeholders across the Department.

Goal 3: Expand Innovation

To sustain a robust technology portfolio, we will continue to assess and integrate applications that enhance our capabilities and build capacity. Also, we will bolster our standard operating procedures, business processes, and policies to judiciously achieve our goals, especially as they relate to using AI and other emerging technologies. Innovation will be integrated into how we support DOJ Components, provide services, manage data, and make technology decisions.

Goal 4: Advance the Workforce

The Department will strengthen its workforce by leveraging information to identify skill gaps, track employee capabilities, and align talent with mission priorities. By using data-driven insights to enhance hiring, retention, and training strategies, DOJ will continue to build a diverse, adaptable workforce equipped to meet evolving challenges and mission priorities.

Goal 5: Increase Financial Transparency

DOJ's efficient management of IT expenditures, combined with stringent investment and budget practices, will allow full use of current tools, enable increases in future technology investments, identify opportunities to reduce expenses, and bolster contract administration. We will continue to augment our procedures to enhance financial data governance and improve oversight of IT initiatives and procurements. Through collaboration with our DOJ partners, we will confirm IT investments are managed effectively throughout the Department's budgeting processes.

During the creation of the DOJ IT Strategic Plan, the following two themes emerged: advancing capabilities in Artificial Intelligence and enhancing Data Stewardship across the organization. These themes influenced the goals and objectives and are integrated into many key strategic initiatives. Improving our Artificial Intelligence and Data Stewardship capacity will enable achievement of our mission and vision and will be reflected in the Department's IT investment decisions over the next three fiscal years.

Artificial Intelligence (AI)

As part of OCIO's continued adoption of AI, we must evolve and reinforce our AI strategy and governance, ensuring AI implementations are executed in a safe and secure manner. We recognize that successful AI or emerging technology implementations hinge on addressing clearly defined problems and identifying the optimal solution that achieves mission outcomes. As AI use grows and expands in industry, federal agencies will need to assess the uses and applications for AI while also adapting policies and governance. We have a strong foundation in place at DOJ for continued expansion of AI adoption with necessary safeguards. Implementing a well-planned AI ecosystem will provide a considerable return on investment to the Department by supporting customer IT needs, maturing technical capabilities, increasing productivity, and optimizing development time and costs.

Data Stewardship

As OCIO enhances its data quality policies and procedures, it will also make measurable progress on leveraging data to improve IT operations and building new data capabilities and tools to enable the Department to execute the mission more effectively. Concurrently, OCIO will maintain strong data security and usage policies, including well-defined rules and procedures that assure the integrity of the data used and protect it from security threats. It is critical to have a systematic and scalable approach to enable data reuse, securely manage multiple data sources, develop new data management tools and capabilities, and protect the integrity of our data. OCIO must enhance its enterprise data policies to enable comprehensive data catalogs and reduce siloed data ownership by establishing systems of record. Furthermore, optimizing the data classification requirements that are assigned to all data elements in the technology portfolio and creating a data governance framework will ensure consistent application of policy and compliance with regulatory and ethical standards. As the Department's designated data steward, OCIO will continue to optimize management processes, enhance data security, increase operational efficiency, and expand data services.

OCIO will engage DOJ Components to implement the DOJ IT Strategic Plan and continue to support the collaboration required to maintain high-performing IT services that benefit both internal and external stakeholders while enabling the Department's mission.

Goals & Objectives

Goal 1: Enhance Service Delivery

Objective 1.1: Establish a customer-centric culture that delivers services to 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: Develop innovative capabilities and service offerings to enhance mission operations

Objective 1.4: Define and standardize communications processes to support communications with stakeholders

Goal 2: Elevate Cybersecurity

Objective 2.1: Reinforce DOJ's cybersecurity foundation

Objective 2.2: Implement Zero Trust principles and tools to combat identity and access-based threats and harden 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

Objective 2.5: Evolve cybersecurity capabilities to prepare for emerging technologies

Goal 3: Expand Innovation

Objective 3.1: Optimize infrastructure and application portfolios and create design standards to improve the digital customer experience

Objective 3.2: Implement AI and intelligent automation to enhance productivity and efficiency

Objective 3.3: Enhance data stewardship, sharing, and governance standards to maximize value of information assets and enable collaboration

Goal 4: Advance 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: Enhance human capital management tools to effectively develop the workforce

Goal 5: Increase Financial Transparency

Objective 5.1: Standardize financial management practices so that DOJ can gain greater insight into IT costs and budget tracking

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

Goal 1: Enhance Service Delivery

We are committed to always providing an exceptional customer experience and deploying tools to help mission staff increase their productivity. By delivering this experience through excellent, customer-focused services, we will enable our workforce to advance DOJ's law enforcement and litigation capabilities and grow confidence throughout the Department in dependable IT support and services. We will achieve this by leveraging the voice of the customer, holding vendors accountable, and monitoring services to provide rapid responses and attain optimal operational stability. In addition, we will continue to bolster our communications processes so that all stakeholders receive clear and consistent communications.

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

As technology is embedded into every aspect of the Department's mission and as customer experience is a priority, we must maintain a culture of service delivery that focuses on creating an excellent experience for our customers.

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

The voice of the customer will continue to play a central role in understanding where DOJ services and customer engagement can be improved. We will also enhance our customer centric culture to understand where services could be optimized and how user experience could be improved to benefit customers. We plan to continue leveraging modern user-centered design concepts to holistically address the full range of graphic, interface, and human-centered design methodologies when delivering digital products. By consistently examining service delivery and incorporating leading practices, our service offerings will be improved to match industry standards and add business value.

Expected Benefit: DOJ IT Services will constantly improve delivery methods and drive effective stakeholder engagement to meet customer needs.

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

OCIO is responsible for ensuring the services we contract from providers and the services offered to our customers are dependable, resilient, and transparent. Especially after large-scale cyber-attacks or outages, DOJ must closely monitor services to detect abnormalities or deficiencies. Building on our service management efforts and ISO 20000 certification, we will continue to collaborate with partners and customers to deliver high quality IT services.

Initiative 1.2.1: Increase service resiliency

To meet the Department's mission, it is essential to operate with minimal service disruptions. To avoid unpredictable or repeat service failures, we must enhance our service management practices, such as leveraging Information Technology Infrastructure Library (ITIL) standards to build infrastructure that is of the highest quality and incorporating leading practices to drive continuous improvements. Identifying, developing, tailoring, and implementing ITIL principles, specifically around service delivery and support, will enhance DOJ's service management and IT infrastructure capabilities. Services that are resilient and flexible will decrease downtime and allow DOJ to remain operational in case of unexpected outages.

Initiative 1.2.2: Enhance consistent delivery methodologies

DOJ must continuously augment its delivery methodologies to improve its ability to provide reliable services and mitigate risks that could cause disruptions in service or result in a security breach. We will expand the use of enterprise cloud platforms and solutions modeled on shared responsibilities, as well as monitoring capabilities to provide more robust and scalable solutions. In addition, we must continue to analyze and increase useability, accessibility, and resiliency for each of our systems and applications. Through additional visibility into the performance of services, we can decrease disruptions, validate that metrics meet or exceed performance standards, and ensure that any irregularities are identified and mitigated quickly.

Initiative 1.2.3: Enhance vendor accountability

As a consumer of commercial services and products, such as eLitigation, eDiscovery, and cloud products, DOJ works with vendors to deliver effective and efficient services. We will establish Enterprise License Agreements for high-demand commodity cloud services and create enforceable Service Level Agreements (SLAs) for services that are currently not in place or sufficiently robust. This will allow us to act as customer liaisons while holding vendors accountable to a comprehensive set of measures, duties, and expectations.

Expected Benefit: OCIO will continue to implement industry-leading practices that enhance reliability of services, reduce downtime, and increase visibility into costs and performance.

Objective 1.3: Develop innovative capabilities and service offerings to enhance mission operations

In a changing digital landscape, we need enhanced technology capabilities to accomplish mission activities. Powerful new IT tools make it simpler than ever to discover insights and keep pace with the expansion of digital information that is available. Improving capabilities and services will allow DOJ to better accomplish its law enforcement activities, mitigate threats, and hold bad actors responsible. These capabilities and offerings will harness innovation and transform processes to be more efficient, while creating new products or services that deliver better value.

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

Our mission staff leverage cloud-based solutions to deliver modern electronic-litigation and case management capabilities intended to keep pace with the velocity of the current litigation landscape. We will partner with mission stakeholders to develop these capabilities using industry leading practices. In addition, DOJ must increase the use of data analytics platforms, capturing large volumes of data while delivering consistent data sharing, analytic and visualization capabilities to better support decision makers. OCIO will keep working with our partners across the agency to help the Department achieve its mission.

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 enhance our service offerings, we will continue to improve the management of DOJ wireless spectrum requirements to ensure law enforcement missions maintain the tactical communications capabilities necessary to meet mission needs. We will also strengthen our biometric capabilities to deliver a modernized and integrated solution to support Federal, State, Local, Territorial, and Tribal law enforcement agency data sharing and access requirements 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.

Initiative 1.3.3: Increase the adoption of emerging technology to solve critical mission problems

DOJ is working to implement shared test and production AI platforms and tools by leveraging cloud solutions, modern data, and application expertise, as well as multi-disciplinary governance models to enhance efficiency while addressing privacy and safety concerns. The Department constantly assesses new technology to offer to all Components as part of a shared service model to address common requirements and business needs. In addition, DOJ will leverage 5G and edge computing technology to deliver improved real-time data processing and communication capabilities across the enterprise. Also, the Department will

continue moving towards software-defined networking and greater use of cloud brokerage services to increase the sharing of data across the organization. These efforts will help increase efficiency and effectiveness, reduce risk across the organization, and better meet mission needs.

Expected Benefit: DOJ will create new services and augment existing ones in a timely manner to continuously assess and improve mission operations.

Objective 1.4: Define and standardize communication processes to support communications with stakeholders

In a constantly changing digital landscape, we need to ensure that all stakeholders understand how they will receive information, when they should expect it, and what actions they should take after getting it. OCIO collaborates with many stakeholders with differing missions, making effective and timely communications critical to achieving success across the Department.

Initiative 1.4.1: Develop unified brand and Strategic Communications Plan of Action to engage with customers to provide a standard and consistent digital experience

As the pace of digital interactions across the Department increases, OCIO must equip its customers with updated information so they can make accurate decisions in a timely manner. OCIO will require all service owners to establish a web presence to market their services and communicate via their website with customers. This communication channel will help customers understand who the service owners are and engage with them directly to resolve service-related issues quickly. In addition, OCIO will ensure all service owners engage with the Communications Team before creating communication materials. Further, all service owners will be provided with guidance on standardization and how to effectively communicate with customers. Standardized communications will strengthen OCIO's credibility and allow customers to have a consistent experience. DOJ Components are also standardizing communications with users of IT services and products. The United States Marshals Service (USMS) is keeping customers informed and engaged through an enterprise intranet messaging service and reviewing improvement opportunities to streamline communications with customers.

Expected Benefit: DOJ stakeholders will have aligned expectations for their experience and greater trust in IT services and products.

Goal 2: Elevate Cybersecurity

DOJ must be a standard of excellence for cybersecurity to effectively support our mission and our stakeholders who rely on us for cyber capabilities. We must drive our cybersecurity and identity practices to address challenges within the Department. These challenges include vulnerabilities introduced by the increased use of cloud technology, the evolving landscape of IT supply chain risks, and the need for advanced threat detection and response mechanisms. We must strengthen our security posture against complex cybersecurity attacks, improve and fortify internal remote access for our mobile workforce, enhance our cloud security and monitoring capabilities, secure our IT supply chains, and leverage advanced technologies to better prepare ourselves for the future.

Objective 2.1: Reinforce DOJ's cybersecurity foundation

The Department will continue to improve its asset management processes and tools and use automation capabilities to track inventory and assets. DOJ will bolster its Trusted Internet Connection (TIC) capability based on Zero Trust Architecture (ZTA) principles. DOJ must also ensure its management of vulnerabilities is compliant with federal mandates, including reducing and managing risk of legacy Plans of Action and Milestones (POA&Ms) and end-of-life software. DOJ will work with internal stakeholders to add a clause to all future vendor contracts that requires vendors to meet DOJ cybersecurity standards.

Initiative 2.1.1: Enhance asset inventory management

DOJ will continue to strengthen its asset management processes and tools, as well as utilize automation capabilities to manage inventory and solutions. 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 key safeguard to protect DOJ from cyber-attacks and enhance our awareness of potential risks. To better manage assets, DOJ will enforce the persistent deployment and management of Endpoint Lifecycle Management System (ELMS) agents to every laptop, desktop, and server, as well as scan 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.

Initiative 2.1.2: Modernize monitoring and management of internet traffic

DOJ will enhance the TIC capability based on ZTA principles, and this approach will support our foundational tools while evolving the DOJ cybersecurity program. Although the traditional TIC scope and purpose will be reduced through the adoption of ZTA, the TIC will continue to support on-premises technology, inbound traffic for public-facing systems, and our operations during the transition to a full ZTA model. Implementing ZTA allows DOJ to modernize the monitoring and management of internet traffic, further fortifying DOJ's adaptive cybersecurity posture.

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

DOJ must ensure the management of vulnerabilities is compliant with federal mandates related to risk reduction, through decreasing and managing risk of legacy POA&Ms and end-of-life software. The ELMS will provide an enhanced view of all software and inventory to determine 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 information gathered from ELMS. 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 based on 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 enhance its penetration testing capabilities by conducting ground truth testing for all systems to enable DOJ to proactively reduce risks and mitigate vulnerabilities.

Initiative 2.1.4: Improve Vendor Security Contract Requirements

DOJ will support procurement to include a clause in all future vendor contracts that requires providers to meet DOJ cybersecurity standards. This includes implementing data protection measures when processing, storing, and transmitting DOJ information. By embedding these requirements into vendor contracts, we aim to ensure that all third-party service providers adhere to the robust DOJ security standards, thereby safeguarding sensitive DOJ data and maintaining the integrity of the DOJ cybersecurity framework.

Expected Benefit: DOJ will better manage its threats and reduce risk to the Department by fully utilizing its strong foundation of tools, capabilities, and policies.

Objective 2.2: Implement Zero Trust principles and tools to combat identity and access-based threats and harden information systems

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, DOJ must continue to modernize its approach to cybersecurity. Large-scale security breaches and supply chain attacks from foreign nation states highlight the need to accelerate our cybersecurity efforts through transitioning to a Zero Trust Architecture (ZTA). ZTA is a comprehensive approach to cybersecurity based on the principle of never trust, always verify. It eliminates implicit trust, requiring a contextual approach that considers the application, user, and device to make access decisions dynamically.

To address these threats, over the next three years DOJ will focus on several key ZTA initiatives. We will unify departmental identity providers into DOJLogin and integrate all Components applications for streamlined authentication. This centralization will reduce vulnerabilities and administrative burdens to enhance collaboration across the Department. We will deploy and maintain a Zero Trust Broker for DOJ assets, using identity attributes and dynamic access policies. Additionally, we will implement micro-segmentation, granular management policies, and conditional access policies to support our ZTA transition.

Further, we will utilize automated Endpoint Detection and Response, Mobile Threat Defense, and security orchestration to strengthen our threat detection, response, and remediation capabilities. By adopting these Zero Trust principles and tools, DOJ aims to significantly improve its security posture, safeguard our systems, and enhance our overall cyber defense strategy.

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 unifying departmental identity providers into DOJLogin. As part of our process to centralize our Identity Providers (IdPs), we will integrate all Component applications with DOJLogin for authentication. Users will be required to authenticate using a Personal Identity Verification (PIV) credential, with strong credential issuance and non-PIV multifactor authentication temporarily permitted 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 identity and access-based threats while improving user experience

DOJ will deploy and maintain a Zero Trust Broker for all DOJ assets, utilizing identity attributes, dynamic access policies, and strong credentials. By implementing micro-segmentation, granular management policies, and conditional access procedures, we will continue to build upon our ZTA transition. Leveraging leading technology, we will create risk scores based on several conditions to allow or disallow access, providing baseline scores for conditional access. This approach will enhance our ZTA governance structure and our

ability to track Department-wide progress. DOJ Components are also prioritizing reducing risk through access management solutions. USMS, for example, is investing in capabilities to manage privileges for approved applications. We will also continue to coordinate the transition off legacy networks to Internet Protocol 6 (IPv6), ensuring modern network innovation and performance benefits. Developing thresholds for access and remediation plans will improve user experience while mitigating internal and external threats.

Initiative 2.2.3: Strengthen threat detection, response, and remediation

We will use a rigorous and systematic process to enforce the persistent deployment of endpoint security agents (e.g., Endpoint Detection and Response, Mobile Threat Defense) to all devices, including mobile, in the DOJ environment. Additionally, we will implement security orchestration, automation, and response to streamline and enhance our threat detection and incident response capabilities. This approach 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 expand its ZTA approach to enhance cybersecurity, reduce access risks, better protect against cyber-attacks, and enable timely detection and remediation or potential breaches.

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

As DOJ expands its use of cloud technology, it is important to do so strategically to prevent, detect, and respond to cyber threats. To protect cloud data, the Department will need to closely monitor and manage cloud accounts and services while incorporating advanced security measures. Our efforts will focus on key activities such as improving the cloud system inventory, conducting thorough security assessments, enhancing cloud service provider (CSP) security capabilities, and integrating cloud services with DOJ's unified identity and access management system.

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

We will enhance the Department's cloud system inventory to include cloud service instance metadata and provide comprehensive tracking of our cloud utilization. To enhance security, we will perform agnostic security assessment, monitoring, and incident response through Enterprise third-party Cloud Native Application Protection Platform (CNAPP) tools. Additionally, we will augment cloud service provider native capabilities with interoperable third-party tools to mitigate CSP-specific gaps and establish consistent policy and compliance across a multi-cloud operating environment. Integrating all cloud services usage with DOJ's Unified Identity Provider (DOJLogin) and Privileged Access Management (DOJPAM), as part of the enterprise zero trust architecture will further secure access to our

cloud services. Execution of this approach will increase visibility, security, and management of DOJ's cloud assets.

Expected Benefit: DOJ will have a more secure cloud environment.

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

DOJ will enhance its IT supply chain management by identifying products in the supply chain that support mission-critical operations, developing an approach to manage them, and implementing continuous monitoring practices. We will identify and mitigate risks associated with our vendors and their products to enhance the security of mission-critical systems. By integrating these measures into our procurement and operational processes, DOJ will prevent cyber-attacks, mitigate the likelihood of breaches, and reduce overall risk to the Department by better managing our critical assets.

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

We will document the most mission-critical supply chains by identifying vendors who support DOJ's mission-essential systems. To manage the risk for these supply chains, we will conduct assessments and monitor cyber threat intelligence for these vendors. We will use tools to generate reports in Security Posture Dashboard (SPDR) that show critical software, map supply chain ratings for these vendors, and identify where across the Department the solution is being used. This process will eventually expand to include all software at the Department, and risk scores will be automated and incorporated into SPDR. DOJ will also respond to and mitigate identified risks within the supply chain, while also continuously monitoring for data breaches and threats affecting vendors related to DOJ.

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

The Department will use its software and vendor inventory to develop an enterprise-wide view of the IT supply chain and the risks associated with it. To achieve this, we will establish a continuous monitoring process for the IT supply chain, identifying and assessing risks associated with our vendors and their products. DOJ will create processes and tools to conduct this effort, leveraging existing solutions like SPDR and creating new ones where needed. These tools will enable DOJ to pinpoint potential risks in the supply chain by identifying which Components are utilizing specific vendors, understanding the risk scores of these providers, recognizing which systems might be vulnerable, and determining necessary actions to mitigate these risks.

We will enhance our IT investment and Acquisition Review (ITAR) procedures to ensure that we can identify IT procurements with elevated supply chain risks early in the acquisition

process. By doing so, we will improve our ability to mitigate these risks effectively. Furthermore, we will work closely with our federal partners to exchange supply chain risk information and collaborate on strategies to reduce these risks. This collaborative approach will better prepare DOJ to adhere to new National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidelines and regulations, providing comprehensive supply chain controls over the coming years. DOJ OCIO will also partner with Component System Owners and Authorizing Officials to implement these new supply chain controls, thereby safeguarding our assets while also securing the IT environment.

Expected Benefit: DOJ will be able to better identify vulnerabilities that may exist, avert cyber-attacks and breaches, and decrease the overall risk to the organization.

Objective 2.5: Evolve cybersecurity capabilities to prepare for emerging technologies

As DOJ expands its use of new technology, we must evolve our cybersecurity processes and capabilities to ensure safe adoption and expansion of AI and quantum technologies. We must understand and identify what technology will be susceptible to post-quantum threats and ensure AI is undergoing the same cybersecurity reviews as other technology the Department implements and uses.

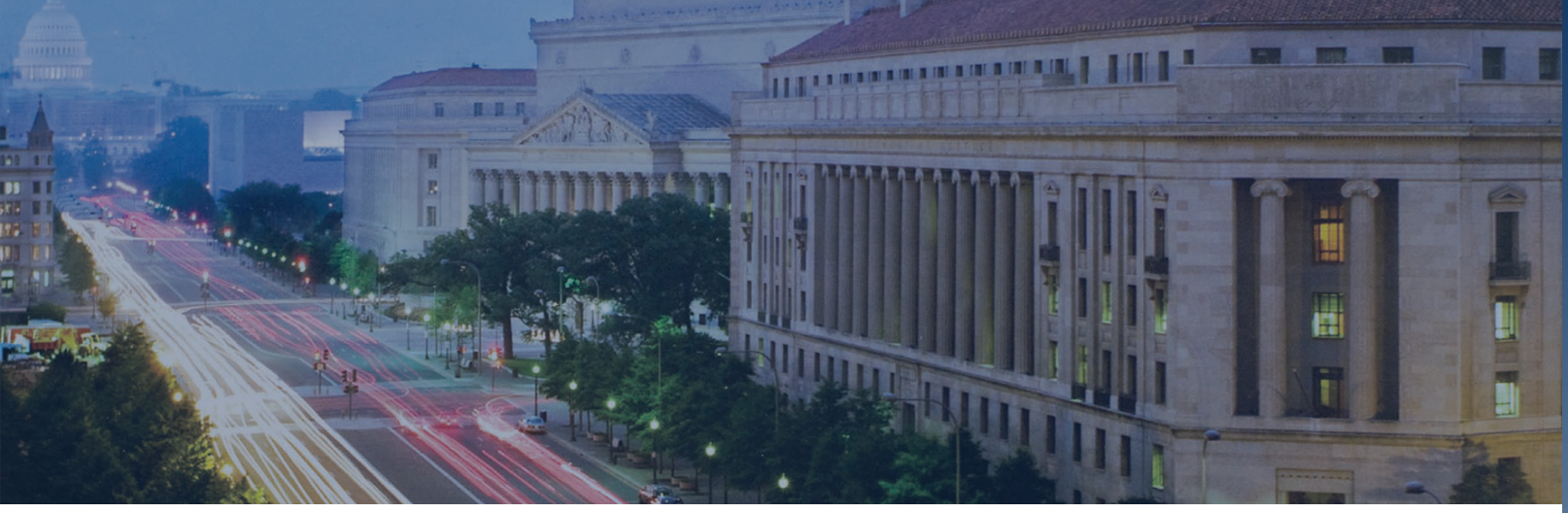
Initiative 2.5.1: Identify post-quantum cybersecurity impacts

We will manage the inventory of cryptographic systems currently in use by DOJ and identify which systems will be vulnerable to post-quantum threats. To support this initiative, we will create a roadmap outlining the steps needed to mitigate the risks from quantum technologies. By proactively managing the cryptographic inventory and planning for post-quantum security, DOJ will be prepared to address future post-quantum threats.

Initiative 2.5.2: Leverage AI to enhance cybersecurity and ensure AI is properly safeguarded

DOJ will align our cybersecurity efforts with the Department's AI policy to ensure AI is following standard cybersecurity processes and practices. We need to safeguard AI just like we do other technologies. We will also use AI to enhance our threat detection and response capabilities. By leveraging AI, DOJ will strengthen our cybersecurity defenses and improve our ability to manage cyber risks.

Expected Benefit: DOJ will reduce risk and protect against future impacts by developing strategies to mitigate emerging technology threats.



Goal 3: Expand Innovation

To maintain a strong technology portfolio, we will rigorously evaluate and implement tools that improve our capabilities and operations. To continue to innovate, we must also invest in our processes and resources strategically and critically to accomplish our objectives. Our people and processes are just as important to innovation as new technology. We must continue enhancing how DOJ manages its data, which will allow more opportunities to make informed decisions, expand the use of AI, and help complete litigation and law enforcement activities rapidly and effectively.

Objective 3.1: Optimize infrastructure and application portfolios and create design standards to improve the digital customer experience

Mission-critical capabilities and technologies must meet the evolving challenges DOJ faces. DOJ must maintain a modern IT infrastructure that is completely capable of sustaining the mission and robust enough to ensure operational effectiveness.

Initiative 3.1.1: Optimize cloud-based technology to ensure the most effective software and hardware portfolio

As stewards of our IT investments, we will continue optimizing our cloud assets and practice efficient multi-hybrid cloud management. We will continue implementing the Cloud Smart Policy along with an enterprise policy, technology standards, and administration of procurement vehicles that are optimized for cloud adoption. We will expand our centralized shared cloud contracts with major providers, so all Components have access to affordable services. Many of our Components have migrated to the cloud, and our focus has shifted to optimizing our operations in that environment. As Components grow their technology stacks in the cloud, they must optimize their resources, review and manage costs through financial optimization, and engage in application rationalization processes. We need to continue discarding redundant, outdated, or overly resource-intensive applications. Fewer application management responsibilities will allow DOJ to focus on enhancing service delivery by augmenting our remaining applications.

Initiative 3.1.2: Institute Agile methodologies within the ITIL framework for 100% of system development and implementation initiatives

In a rapidly evolving environment, DOJ must be adaptable while also operating within a framework that emphasizes optimizing service management processes. As the Department modernizes its systems, it must integrate Agile and ITIL throughout the software development lifecycle to ensure a flexible approach to development while also being structured and process oriented. Procurement is an important area for DOJ, and we must ensure that contract personnel are trained in Agile and ITIL through contract language and modification.

Initiative 3.1.3: Implement digital experience standards for all services

As the prevalence of shared services increases across DOJ, customers must have a high-quality and consistent experience each time. As an organization, we must develop digital experience standards and guidelines for all development efforts especially customer-facing applications. By adhering to a set of requirements and frameworks during the development phase, we reduce the likelihood of customer complaints and mitigate the risk of having to rework applications. In addition, we will collaborate with vendors to include the digital experience standards in the services they deliver. Regardless of where a tool is constructed or which service our customers use, their experience with OCIO must be consistent with our standards.

Expected Benefit: DOJ's applications and infrastructure will efficiently deliver mission-critical capabilities, maximize cloud benefits, and ensure a robust IT infrastructure that adapts to evolving demands.

Objective 3.2: Implement AI and intelligent automation to enhance productivity and efficiency

We operate in a dynamic environment that requires us to adjust constantly to remain at the forefront of transformational change. DOJ must have the tools and infrastructure to drive adoption of emerging technology. Intelligent automation such as AI and Robotic Process Automation (RPA) offer the Department opportunities to improve the way we work and how we achieve our mission. The Department can use AI to rapidly redact sensitive items within audio, video, and image-based evidence, and help eDiscovery teams to transcribe, translate, and perform object detection across enormous amounts of audio, video, and text-based data files. RPA has been used at the Department to decrease process times for repetitive and highly labor-intensive tasks such as assessing failed logon attempts and examining server failures saving our teams hundreds of hours of work annually. As we benefit from these new technologies, we must also acknowledge their public safety consequences. Our efforts to deploy intelligent automation depend on our ability to improve our workforce and its skills, collaborate on the application of use cases, and construct policies and guidance to reduce risk. We will follow the guidelines detailed in the Department's AI Strategy and Data Strategy, while conforming with federal mandates and policies related to AI.

Initiative 3.2.1: Support use case development and adoption of ethical AI and other automation practices and tools

Organizations accelerate innovation via focused exploration to assess which tools and technologies could add value. We will build a culture, systems, personnel, and policy that enable experimentation and testing for new capabilities, including AI, across the Department. This will ease the use of new solutions among stakeholders to better support the mission.

To confirm DOJ adopts ethical AI practices based on existing statute, policy, mission, civil rights considerations, and to comply with Executive Order (EO) on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110), we will continue to compile, review, and update our AI Use Case inventory. We will also continue to categorize manual and time-intensive procedures (e.g., financial management, records management, cybersecurity reporting and monitoring, and service delivery monitoring) to evaluate use cases and goals for automation and AI-augmentation.

To better prepare the workforce with technical standards and decision aids for AI, RPA, and other new technologies, the AI Community of Interest and the Innovation Engineering group will continue leading the identification of use cases for intelligent automation. They will also deploy automation technologies or procedures that will improve operations and champion their implementation. To support this, DOJ is constructing a test bed for AI that is cost-effective and scalable. The test bed will be used across DOJ to provide access to AI datasets, algorithms, and tools that can be shared across Component staff. Staff will have the opportunity to experiment, learn, exchange information, and enhance their skills and knowledge.

Expected Benefit: DOJ will use automation and AI to maximize effectiveness, increase productivity, and inform decision-making.

Objective 3.3: Enhance data stewardship, sharing, and governance standards to maximize value of information assets and enable collaboration

We are augmenting the way DOJ tracks its data, who is utilizing the data, what the data is being used for, and how the data should be secured. DOJ has been employing a governance structure to standardize how Components evaluate, send, and receive data across DOJ. We will continue to improve governance, which will reduce gaps in data sharing and expand our ability to get the most value out of our data.

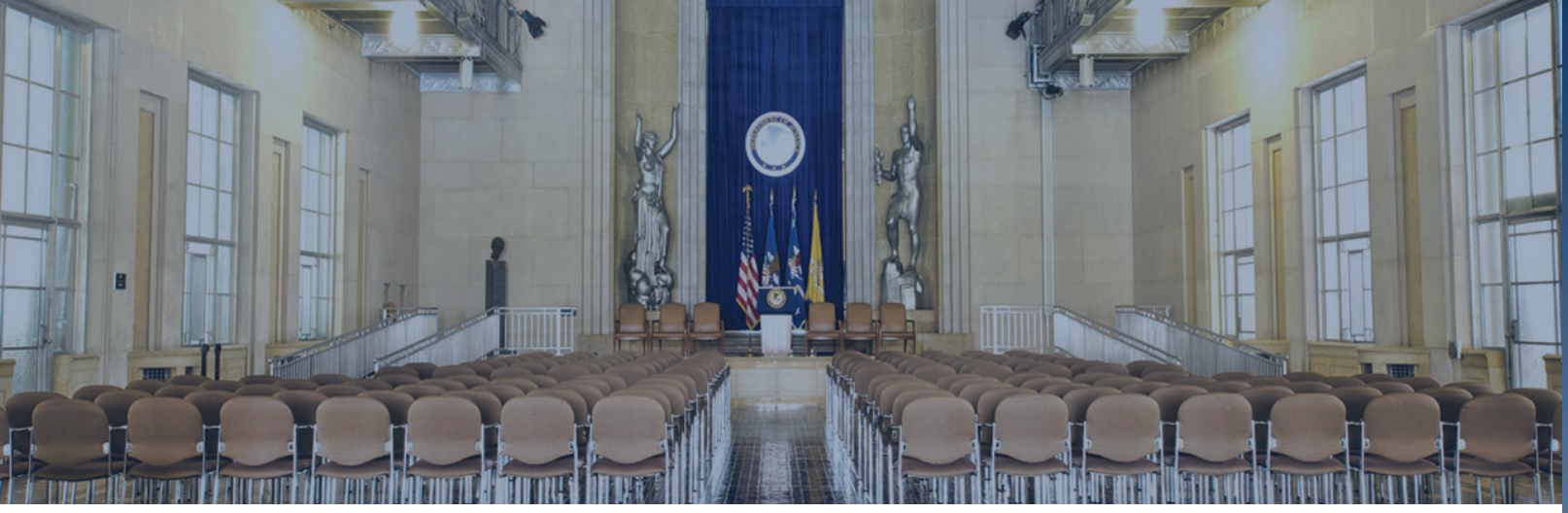
Initiative 3.3.1: Continue to improve data governance, sharing, and collaboration to build a strong foundation for data analytics

To ensure that data inventory is comprehensive, precise, and appropriate, we will continue to communicate the purpose and value of it proactively and continuously to all of DOJ, while also expanding the inventory with key attributes. We will also develop a process for

metadata management and data lifecycle management through the Data Strategy efforts. The management and organization of data assets to successfully use analytics will enable informed decisions in mission areas such as litigation and law enforcement.

To create Department-wide guidelines and leading practices for data governance and data sharing, DOJ will identify and circulate data exchange standards and practices, including inventory and risk assessment requirements for data exchange with assistance from the Data Governance Board (DGB). We will also construct a data exchange framework for Components to record, validate, and standardize how information is shared. An inventory of data exchanges will be retained within DOJ's data repository. Through the implementation of DOJ's Data Strategy and Geospatial Data Strategy, we will continue to improve compliance with open data requirements and decrease barriers for the public to find and analyze data. We will use public engagement for our important datasets and enhance value by hosting challenges. The Federal Bureau of Prisons (BOP) is implementing a multi-year data transformation initiative to advance BOP into an organization that uses data as a critical part of its decision-making processes. This BOP project includes analyzing data to inform evidence-based decisions to improve agency operations, ensuring real-time data capabilities can support preventative and corrective actions, and confirming data is accurate and accessible to increase transparency and comprehension.

Expected Benefit: DOJ will securely and effectively share, access, and use data critical for investigation and litigation mission activities across DOJ and with the broader government and public as appropriate.



Goal 4: Advance the Workforce

By attracting and maintaining a talented and diverse workforce that has the experience, skills, and tools required to excel in their roles, DOJ will drive the mission forward with agile and knowledgeable personnel. We need to cultivate a workforce that is empowered to adjust to the unexpected, develop new skills, and prioritize mission success. As an organization, we must continuously enhance our retention and recruitment strategies to build and retain a capable, diverse, and talented workforce. In addition, we must continue to have an environment that encourages all employees to understand their current capabilities and work towards improving their skills.

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

We are investing in strategic retention and recruitment practices over the next three years to cultivate and retain a diverse IT workforce. Currently, the Department has several vacancies for IT positions and our staffing level is below the desired threshold. Various factors contribute to this challenge, including difficulty finding candidates with the required capabilities and experiences. To address these issues, we are partnering with the Office of Human Resources and Administration (OHRA) and other areas of the Department to attract, grow, and maintain the IT workforce required to be successful.

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

The Department must attract a strong workforce that has the skills critical to advance the DOJ mission. We will continue working with OHRA to construct and manage a position description library to support recruitment efforts and clearly highlight the importance of each role such as mission impact, work life balance, stability, a diverse and inclusive environment, and other benefits unique to the public sector. In addition, we will explore opportunities to use AI to build position descriptions and house them in a repository to enable managers to streamline the hiring process. We will continue coordinating with OHRA to examine the recruiting process holistically to ensure the pipeline reflects our country, while also having

in-demand capabilities, such as expertise in cyber and cloud, as well as participating in job fairs. Further, we will look for ways to broaden our recruitment practices beyond USAJobs.

Initiative 4.1.2: Enhance retention activities to maintain a strong workforce

For DOJ to be a top choice employer with high employee engagement, we must strive to always enhance our personnel experience. We will continue seeking feedback to understand current employee sentiment, capture identified areas for improvement, and create action plans to strengthen engagement. We will also collaborate with OHRA to better describe the career model for IT positions that lay out a clear path to help professionals advance their career. This will increase understanding of position expectations and provide greater openness about career paths. For example, BOP is undergoing a transformation of its IT services and is focused on creating clear career trajectories for IT staff with a goal of improving retention and succession planning. We will also better communicate our current benefits so that candidates are aware of DOJ's student loan assistance and retention incentives.

Expected Benefit: DOJ will meet mission workload demands by increasing staff retention efforts and developing a stronger pool of technical talent.

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

To apply emerging technologies to DOJ operations, we need a workforce with the capabilities to use them. We are devoted to making the investments to continue developing a talented and diverse workforce with the resources to build these skillsets. We will support our IT project and service managers as they grow their abilities in managing projects and financials, which will enhance our consistency in directing IT project budgets. This will be important for developing the workforce and creating the capabilities DOJ needs.

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

We must ensure that trainings, certifications, skill sets, and resources we need to bolster our workforce capabilities are current and defined. We will work to offer opportunities to all of DOJ through collaborative and cooperative efforts. Our IT project and service managers come with a diverse array of professional experiences, skills, and capabilities. To enable optimal IT operations and consistently follow leading practices in project management, agile methodologies (i.e., Scrum, Scaled Agile Framework [SAFe]), financial management, and vendor management, we will support the building and maintaining of competency throughout our manager population across key capabilities. We will help our key leadership and managers embrace the disruptive, yet proven techniques and tools with industry recognized frameworks and coaching services. We will also provide educational seminars on financial

management, forecasting, service planning, business planning, and service estimating so that our managers have a consistent understanding of delivering IT projects within budget.

Expected Benefit: An operational IT workforce that has the experiences, skills, and capabilities to deliver a secure cybersecurity posture and use emerging technologies to advance the Department's mission.

Objective 4.3: Enhance human capital management tools to effectively develop the workforce

To improve DOJ operations, we must understand and monitor the skills and performance of all employees and create an environment where everyone can excel. We must take a methodical approach to identifying where knowledge gaps exist and create a plan of action to address them. By ensuring our employees have a broad base of knowledge and skills to make them successful in their job, we will advance DOJ's mission.

Initiative 4.3.1: Develop a strategy for human capital management, including inventory, tracking, and performance management tools and processes

We will develop a strategy to enhance the capabilities and skills of all employees. All employees will have access to personal development plans that list their current skills and experiences, describe the next level of capabilities to be acquired, and measure the amount of time it takes to reach it. Whether an employee is at the individual contributor or manager level, they must continue acquiring new skills and experiences. As an organization, we must help manage and track the skills and capabilities of our employees to make sure everyone is growing their skillset and is able to utilize their talents when a new opportunity arises. Proactively managing our most valuable asset, our talent, is critical to DOJ meeting its mission objectives and transforming technology to better position the organization for the future.

Expected Benefit: Proactive development of DOJ employees' skillsets will enhance performance and increase ability to address future challenges.

Goal 5: Increase Financial Transparency

Effective IT financial management integrated with budget and investment tracking will enable DOJ to maximize its technology assets, identify cost optimization opportunities, enhance contract oversight, and ensure our IT capabilities are cost-effective and beneficial. We will implement standards and improved governance practices to strengthen financial stewardship, and better manage IT projects, acquisitions, and budgets. We will also work with our IT partners, DOJ leadership and stakeholders, to ensure IT investments are reviewed and tracked appropriately as part of DOJ's budgeting processes. IT is in everything we do and supports every mission activity, and we need to account for additional necessary investments as independent line items in the budget.

Objective 5.1: Standardize financial management practices so that DOJ can gain greater insight into IT costs and budget tracking

Since the transition to DOJ's Unified Financial Management System (UFMS), the Department must further refine its governance and reporting mechanisms to accurately track IT spending and enable clear visibility into total cost of ownership for IT projects and services.

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

DOJ and its Components have adopted UFMS as the common financial management platform to enable a structured and transparent view into the way DOJ makes IT investments. We will refine OCIO's UFMS associated governance processes to help Components better track IT spending across the Department and to provide an improved understanding of shared service costs. In addition, we will use the Technology Business Management framework to align spending to IT priorities, minimizing capability duplication and maximizing mission support.

Expected Benefit: Enhanced financial management practices will enable data-driven decisions to better align IT resources to mission priorities.

Objective 5.2: Support strong governance of IT investments and acquisitions so 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. By standardizing inventory tracking and improving cost transparency, we will enable DOJ and the Components to have a single, up-to-date view of IT spend to facilitate informed procurement decisions. Automating processes and controls enhances agreement coordination and financial reporting across the Department. DOJ will also leverage shared services and data from prior IT procurements to help avoid redundancies and drive informed decisions when evaluating new technologies.

Initiative 5.2.1: Use prior cost performance and relevant technical requirements to better inform IT acquisitions

The implementation of standardized financial management practices, such as inventory tracking and automation of processes and controls, will enable DOJ and the Components to have a single, up-to-date view of IT spend and will facilitate decision-making as it relates to procurement decisions. In addition, we will continue to automate processes and controls to improve agreement coordination and financial reporting.

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

Promoting the reusability of products and acquisition vehicles for groups of capabilities or service functions across mission areas has allowed the Department to get the best value out of existing solutions. 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, developing category management policies and procedures to reduce contract duplication, highlighting opportunities for cost savings and cost avoidance, and minimizing over/under spend on software licenses. These activities will enable DOJ to scale IT investments to mission needs while also optimizing the allocation of resources. As an example, USMS is planning to implement a new technology platform to meet modern mission requirements and deploy new capabilities through a single contract vehicle that will offer bulk volume discounts and cost-efficiency.

Expected Benefit: A holistic view of IT spend will enable efficient technology investments and optimize resource allocation.

Appendix

The U.S. Department of Justice Information Technology Strategic Plan for Fiscal Years 2025-2027 aligns with the strategic plans listed below.

- **DOJ Strategic Plan for Fiscal Years 2022 – 2026**
- **DOJ Data Strategy**
- **DOJ Geospatial Strategy**
- **DOJ AI Strategy**
- **DOJ IT Strategic Plan for Fiscal years 2022 – 2024**

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 2025 through 2027, there will be annual updates 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.