



Administrative Office
of the United States Courts

Long Range Plan for Information Technology in the Federal Judiciary

Fiscal Year 2027 Update

10/01/2026

Long Range Plan for Information Technology in the Federal Judiciary: Fiscal Year 2027 Update

Table of Contents

Introduction	1
Information Technology Strategic Priorities.....	2
Case Filing/Case Management	3
Case Management Modernization (CMM)	4
Other Case Filing Services	4
Electronic Public Access	5
Jury Management.....	5
Judges and Chambers Staff.....	6
Administrative Support.....	6
Judiciary Data Management and Governance	8
Maximize National Systems through Court-Led Best Practices	10
Enterprise Strategy, Architecture and Innovation	11
Network Enhancements.....	11
National IT Operations	11
Enhanced Hosting Services	12
Courtroom Technologies	12
Communications.....	13
Artificial Intelligence	13
Preventing Malicious Activity	13
Detecting, Analyzing, and Mitigating Intrusions	17
Shaping the Cybersecurity Environment.....	18
Investing in the IT Program	18
Resource Requirements	19
JITF Program Components.....	20

Introduction

The *Strategic Plan for the Federal Judiciary*¹ defines the Judiciary's mission as follows:

“The United States Courts are an independent, national Judiciary providing fair and impartial justice within the jurisdiction conferred by the Constitution and Congress. As an equal branch of government, the federal Judiciary preserves and enhances its core values as the courts meet changing national and local needs.”

Judges and Judiciary staff regard information technology (IT) not as something separate from their day-to-day work, but as an essential means to perform their jobs. As business processes and technology solutions have become interwoven, the Judiciary recognizes that IT plays an indispensable role in the work of the Judiciary and offers opportunities to develop more efficient and effective processes supporting sound and efficient operations.

Pursuant to section [612 of Title 28, United States Code](#), the Director of the Administrative Office of the United States Courts (AO) is responsible for preparing and annually revising the *Long-Range Plan for Information Technology in the Federal Judiciary* (*Long-Range Plan*). The Committee on Information Technology of the Judicial Conference of the United States provides guidance in the development of annual updates and recommends the plan for approval by the Judicial Conference. Upon approval, the Director provides the annual update of this plan to Congress.

This update to the *Long-Range Plan* describes key strategic priorities for enterprise-wide IT over the next three to five years and summarizes the Judiciary's anticipated IT resource requirements for fiscal year (FY) 2027 through FY 2031. The strategic priorities discussed in this document integrate the *Strategic Plan for the Federal Judiciary*, as updated in 2025, with the IT planning and budgeting process and Judiciary-wide strategic planning efforts. The strategic priorities were further informed by discussions within the AO's advisory process, as well as circuit judicial and IT conferences.

The Judiciary's IT program consists of systems and services provided both at the national level and by the courts individually. The program consists primarily of five elements:

- Public-facing technologies that serve the general public, as well as litigants, attorneys, law enforcement agencies, state and local courts, executive branch agencies, and other stakeholders.
- Internal Judiciary systems used by judges and chambers, court staff, probation and pretrial services officers, and AO personnel.
- The technical infrastructure that is the underlying framework supporting the delivery and processing of information for all stakeholders, both internal and external. It includes the physical equipment, network policies, and rulesets that ensure the confidentiality, availability, and integrity of the Judiciary's IT services.
- IT security methods and processes that protect internal and external Judiciary systems, services, and data against unauthorized use, disclosure, modification, damage, inaccessibility, and loss.

¹ [Strategic Plan for the Federal Judiciary](#), approved by the Judicial Conference of the United States, September 2025.

- Enterprise strategy, architecture and innovation practices that guide the strategic alignment of business goals and technology investments, ensure interoperability across Judiciary systems, and foster the adoption of emerging technologies to improve mission effectiveness and operational efficiency.

Information Technology Strategic Priorities

The [Strategic Plan for the Federal Judiciary](#) combines the priority of, “Realizing technology’s full value and managing its risks,” with the need to protect the integrity of the judicial process and the information entrusted to the Judiciary by litigants seeking equal justice under the law. The modern digital environment offers immense opportunities to leverage technologies to provide more timely and efficient access to Judiciary services but also creates new risks as the Judiciary combats emerging threats from criminal and nation-state sponsored cyber actors seeking information on trade secrets, intellectual property, and information pertaining to ongoing investigations. The disclosure, modification, or theft of this information by these outside entities can undermine public confidence in the judicial process and cause irreparable harm to the reputation of the Judiciary. To effectively protect the Judiciary from sophisticated cyber threats, while still enabling public access, the Judiciary must modernize its environment, while still securing the functionality of its legacy systems. This can only be accomplished through the recruitment of new talent and broadening skills of existing staff to take advantage of new capabilities in automation, machine learning, and the cloud. In support of this plan are five associated implementation goals which form the basis of the strategic priorities for IT:

- Ensure that court and national systems are covered by the continuous diagnostics

and mitigation program, which delivers cybersecurity tools, integration services, and dashboards to help improve the judiciary’s security posture.

- Continue to build, maintain, and enhance robust and flexible technology systems and applications that anticipate and respond to the Judiciary’s requirements for efficient communications, record-keeping, electronic case filing, public access, case management, and administrative support. Modernize the Judiciary’s IT infrastructure and systems to ensure continuous system up time for the judiciary’s enterprise systems and public-facing systems.
- Ensure that judiciary IT staff have the necessary skillsets in relevant, cutting-edge technologies through ongoing education programs.
- Establish an AI governance framework to guide responsible adoption of AI and to manage risks and challenges presented by the new and evolving technologies.
- Establish a formal Judiciary Innovation Program that encourages active participation in the innovation of IT systems and applications across the Judiciary by all members of the Judiciary community.

IT is inextricably part of the execution of the Judiciary’s business. Applications to perform case filing, case management, and administrative support are supported by communications and collaboration systems. These systems and applications require ongoing maintenance, improvement, upgrades, and replacement to remain functional in a continually changing external environment as well as relevant to the current needs of the Judiciary. In addition to managing a structured lifecycle-management process to identify, manage, and implement user requests for system improvements, the Judiciary regularly assesses whether business

needs or new technologies necessitate more extensive upgrades or even full replacement of existing systems. The Judiciary currently dedicates most of its IT resources to sustaining legacy (sometimes outdated) technologies but, to take advantage of technology advances and to protect the Judiciary from cyberattacks, the Judiciary must take measured steps to modernize its IT environment. Descriptions of anticipated system and application changes are provided as examples of this planning process in action and to delineate the areas on which the Judiciary will place priority over the next three to five years.

The *Judiciary IT Modernization and Cybersecurity Strategy*, published in September 2022, sets the framework for evolving the Judiciary into an organization that operates as a united, trained, flexible, security-first workforce utilizing secure, modern, standardized technologies to meet the rapidly changing needs of the courts. Work on several foundational modernization initiatives is ongoing, such as modernizing the Judiciary's identity management systems, network infrastructure, authentication and access management systems, and several critical business systems. Additionally, efforts are underway to establish the enterprise architecture function and to establish enterprise technical standards, which will help drive uniformity across the technology framework of the Judiciary. Currently all modernization initiatives are closely monitored to ensure the appropriate level of progress is being made in achieving the outcomes expected for each initiative.

The following sections describe significant initiatives that are planned over the next three to five years to address each of these strategic goals.

Case Filing/Case Management

Case Management/Electronic Case Files (CM/ECF): The federal courts' case filing processes occur within the CM/ECF system, through which court staff and attorneys open cases and file documents over the internet. Case information and related documents are electronically available to case participants at virtually the same moment a filing is completed. Nearly instantaneous email notification of any activity in a case maximizes the time available for participants to respond. These efficiencies have reduced the time and cost required for litigants to work through the judicial process. The public benefits from electronic case information and document availability through the PACER service as a result of the CM/ECF filing process.

The implementation of Next Generation (NextGen) CM/ECF modernized the business processes used by the courts and judges' chambers. NextGen CM/ECF enhanced the way judges manage cases by streamlining their processes and the ways they view information in the application. NextGen CM/ECF also enabled judges, court staff, and attorneys to access CM/ECF data in multiple courts using a single account; provides appellate attorney filers with a new, streamlined interface; enhanced the Judiciary's ability to exchange data within its internal and external systems; supported a more consistent user experience for external users; improved filing capabilities for pro se filers in bankruptcy cases; and provided a new, streamlined interface for automatic judge and trustee assignments in bankruptcy cases.

As of September 2022, all courts have transitioned to and are now live on NextGen CM/ECF. Courts continue to upgrade to the latest two supported versions of NextGen CM/ECF. These upgrades improve the Judiciary's CM/ECF security posture. NextGen CM/ECF is currently in "lights on" mode where resources will be available only to continue its

secure operation, with changes or improvements being extremely limited. In “lights on” mode, upgrades and development activities will be limited to zero-day and high vulnerability fixes as well as mandatory changes required by new laws. The existing resources will be required for the ongoing O&M efforts.

Case Management Modernization (CMM)

The AO started the CMM effort to replace CM/ECF with a modern, cloud-based, sustainable platform for the Judiciary to manage cases and improve communication, collaboration, and engagement among courts, the public, and other partners. A modernized system will significantly improve the Judiciary’s cybersecurity posture and benefit not just the courts, but also litigants and the public who seek to access court records. The modernization project incorporates the fundamentals of today’s IT development best practice principles: user-centered design and iterative, agile development based on testing and user feedback. The modernized version of case management will implement modern data standards with a data catalog and data governance framework. Part of the CMM effort includes adding enhanced search functionality to PACER, which will make searching court records more accessible and intuitive. The AO’s CMM program staff are engaging with the court community throughout the effort.

In an effort to accelerate the project, the system will roll out in increments that are phased and prioritized to reduce cyber risk and meet operational needs. As increments are being developed, they are being tested and enhanced by select courts, referred to as pathfinder courts. Pathfinder engagement is necessary and important as it allows the AO to know the new system will meet the operational needs of courts. The first module of the new system is expected to roll out to all

pathfinder courts by the end of calendar year 2026. Additional functionality will then roll out to district courts throughout calendar year 2027 and likely into the first half of 2028.

Other Case Filing Services

Probation and Pretrial Case Tracking System (PACTS): PACTS has evolved into a comprehensive case management system for probation and pretrial services officers and has become an indispensable supervision and investigation tool. In recent years, the AO has implemented changes that have stabilized and ensured the reliability and performance of PACTS and its related applications greatly. PACTS360, which is the replacement system for PACTS, takes advantage of software as a service (SaaS) to provide a highly configurable platform-based solution. The replacement system will continue to interface with key applications, both internal and external to the Judiciary, and provide officers with the data necessary to fulfill their mission. In November 2023, the AO announced a delay in the completion and the rollout planned for FY 2024. After detailed analysis and implementing all the corrective measures, PACTS360 development and testing were completed in January 2026 and was rolled out to four pilot districts on February 23, 2026. With pilot districts now live, program efforts have shifted from deployment readiness to operational stabilization and long-term sustainment planning.

eVoucher and Vendor Manager (Criminal Justice Act (CJA) products): The CJA eVoucher product is the Judiciary’s national application for managing CJA appointments; voucher submission, review, and payment; panel management; service provider authorization; and case budgeting. The eVoucher product integrates with the Judiciary Integrated Financial Management System (JIFMS), enabling all vouchers to be sent automatically to JIFMS for payment upon approval and certification in eVoucher. In March 2025, the Vendor Manager System (VMS) was successfully deployed nationwide, allowing invited Judiciary vendors to manage their own

contact, tax certification, and bank account information. In addition, VMS verifies vendor tax information matches IRS records prior to syncing data with eVoucher and JIFMS, improving compliance with treasury and IRS requirements. Nearly all CJA payments are now sent via electronic fund transfers. Since the release of VMS, over 12,000 unique CJA vendors have registered to receive their payments electronically. In 2025, the team completed assessments to understand migrating eVoucher and VMS to a Judiciary-approved cloud service provider. Human-centered design activities and deliverables were also completed to define the scope of the minimum viable product for future development.

Electronic Public Access

The Judiciary provides electronic access to case information, including the documents in case files, through its Public Access to Court Electronic Records (PACER) service. The public and other external stakeholders do not need to visit courts in person to obtain a case file and photocopy documents. Instead, the program's 5.5 million registered users can obtain these documents and other case information online. At the same time, to strengthen security and protect privacy, the Judiciary has instituted policies and there are federal rules of procedure that restrict electronic public access to certain types of cases, information, and documents. The Judiciary's Electronic Public Access (EPA) program has worked to improve electronic public access to court information and documents through several ongoing initiatives. Many future improvements to electronic public access to court records will be directly tied to the Case Management Modernization (CMM) effort.

EPA Public User Group: In 2020, the AO established a Public User Group—composed of 12 non-Judiciary members representing the legal sector, media, academia, government agencies, and other entities that regularly use PACER—to provide advice and feedback on ways to improve PACER and other electronic

public access services provided by the Judiciary. The group has made several recommendations for improving public access services. The AO has analyzed each recommendation to determine appropriate actions consistent with Judicial Conference policy and technical, legal, and financial feasibility and to determine best approaches for implementation. Recommendations from the group were instrumental in creating functionality improvements in the PACER Case Locator, raising awareness among courts of the importance of implementing CM/ECF RSS (Really Simple Syndication) feeds, and developing a Pro Se User page on the PACER website.

The EPA Public User Group is also playing a role in the Judiciary's effort to modernize CM/ECF and PACER. The group has been actively engaged in the development process of the new PACER interface. The members have participated in regular user research sessions that focused refining requirements for various features of the new system—such as search and case alerts—as the project has advanced through the development lifecycle.

Jury Management

Jury service is an important civic function that supports the right of trial by jury. The right of the accused in criminal prosecutions to trial by jury is protected by the Sixth Amendment to the Constitution and the right to trial by jury in civil common law actions is preserved by the Seventh Amendment to the Constitution. The judiciary's jury management system has three main components that provide courts with (1) the ability to randomly select citizens for jury service, pay attendance fees, and conduct other juror management functions, (2) a vehicle for prospective jurors to submit a statutorily required qualification questionnaire document to the court, and (3) an efficient method to contact jurors with important day-of jury service information and for prospective jurors to contact the court. The AO is working to obtain a cloud-hosted, web-based solution that will be centrally managed, ensuring a more efficient way for the AO to respond to

security vulnerabilities and easing the delivery of future enhancements to the courts.

Judges and Chambers Staff

Although case management systems were originally designed primarily to manage documents and processes in the clerks' offices, NextGen CM/ECF introduced efficiencies to judges' chambers. New features such as the Judge Review Packets provide district and bankruptcy judges and their staff with the ability to automatically create and maintain electronic packets of information for matters that require chamber's review and action. Judges and their staff also can utilize a user interface called Workspace, which provides customizable content based on job function. Mobile Briefcase allows appellate judges and their staff to download and edit documents on a tablet or other mobile device. The Citation Links functionality adds links to PDF documents filed in a case so that judges, law clerks, and court staff can easily view the referenced content using their preferred research resources. With NextGen CM/ECF going into the 'lights on mode' no further updates will be made to the features for the judges and chambers staff. Any new needs will be handled as part of the CMM effort.

Administrative Support

The Judiciary is continuing to modernize and update key national administrative systems supporting finance, human resources, and facilities management. These efforts will deliver high-quality and secure solutions aimed at reducing costs, streamlining operational processes, and strengthening internal controls. The Judiciary's modernization of its administrative IT portfolio strategically aligns with the *Judiciary IT Modernization and Cybersecurity Strategy*.

Judiciary Integrated Financial Management System (JIFMS): JIFMS is a decision support management information system that serves as the Judiciary's official budget, acquisitions, fiscal, and case accounting system of record.

This integrated financial system supports the Judiciary's workflow, internal controls, and financial management functions along with their associated decision support business processes and capabilities. JIFMS interfaces with numerous other federal government systems and is a mission-critical system.

JIFMS was modernized in FY 2025, and improved system security, provided support for the latest infrastructure, and positioned the Judiciary to begin introducing operational efficiencies and enhancements. In addition, the new technical infrastructure and modernized platform will provide the opportunity to leverage advances in robotic process automation, machine learning, and web services.

The Judiciary continues the "back to baseline" strategy, which minimizes Judiciary-specific customization of the underlying commercial solution to streamline operations and maintenance activities and reduce the complexity of future upgrades. Limiting customizations will also help achieve the goal of establishing a routine and predictable upgrade cycle, enabling the Judiciary to take advantage of an up-to-date and supportable financial management solution into the future.

Automated Collections Register (ACR): The AO implemented ACR as a minimum viable product in 2023 focusing on collection modes commonly used inside the data communications network (DCN) (check and over the counter cash/credit card) and incorporating the business requirements of the legacy CA\$H Register and CR/ECF applications. Fiscal years 2024 through 2025 entailed monitoring operations of the MVP while completing the JIFMS upgrade. In FY 2026, the AO will begin development activities to enhance its collection modes to include commonly used services such as PayPal, Venmo, and Zelle. Coordination with The Department of Treasury to introduce service offerings will ensue as a focus will be on developing integrations to afford customers the convenience of paying from additional locations. Offering additional payment access

and convenience will significantly increase collections. This will help to expedite payments to victims and other appropriate recipients.

Debt Management: The Judiciary intends to pursue a unified debt management solution that will replace the Civil/Criminal Accounting Module (CCAM), which is currently integrated into JIFMS, and other debt management solutions used throughout the Judiciary. This new solution will decouple debt management from the core financial system (JIFMS) as part of the “back to baseline” strategy, so that it can stand alone and support the Judiciary’s unique business requirements related to financial accounting, case management, and associated decision support capabilities. It will offer debt management functionality for the district, bankruptcy, and appellate court communities. Efforts to identify and define key business processes will be conducted and documented in FY 2029, with development and implementation activities to follow.

The JIFMS upgrade and future debt management efforts align with a Judiciary strategic effort called the Judiciary Data Integrity, Reporting and Controls (JDIRC) program. JDIRC is a financial management initiative with the goal of submitting a consolidated, audited financial statement to the Treasury Department that is consistent with generally accepted accounting principles. The JDIRC program will transform financial reporting requirements across the Judiciary, improve the Judiciary’s internal controls program, and strengthen the integrity of Judiciary financial data.

Human Resources Management Information System (HRMIS): The Judiciary employs HRMIS to manage key HR transactions, including leave accruals, employee performance management, benefits administration, and payroll processing. Committed to continuous improvement, the Judiciary seeks to maintain the application to the most up-to-date version provided by the software manufacturer and to ensure compliance with regulatory and statutory

requirements. Additionally, the AO collaborates with the court HR community to identify improvements that enhance efficiency, accuracy, and aligns with the workforce planning goals and talent acquisition initiatives.

The HRMIS roadmap includes plans to modernize HRMIS in general by upgrading the PeopleSoft user interface to their latest design standard. In addition, working in concert with AO’s Human Resources Office, there are plans to enhance and modernize specific modules including employment suitability, ePerformance, and Leave Tracking. All these modernization efforts are intended to update functionality to meet changing business needs, improve usability, and eliminate customizations.

Learning Management System (LMS): The Judiciary has established an initiative to enhance the version and scope of the existing LMS. The upgraded, enterprise-wide LMS will more efficiently manage training across the Judiciary. This initiative aligns with the *Strategic Direction of the Administrative Office of the U.S. Courts* to ensure an exemplary workforce and is driven by the Judiciary’s strategic direction of a more unified, adaptable, and well-trained workforce.

The improved LMS will establish a centralized hub for managing, delivering, and tracking all training and learning activities, including the administration of individual learning paths. This centralized platform ensures consistency in training content, minimizes administrative burdens, and provides a foundational platform for all Judiciary learning initiatives.

Financial Disclosure Reporting: The Ethics in Government Act of 1978 requires all judicial officers and certain Judiciary employees to submit financial disclosure reports. To facilitate this process, the Judiciary developed the Judiciary Electronic Filing System (JEFS), a modernized, end-to-end financial disclosure platform designed to meet the needs of filers and administrators. JEPS streamlines the filing and amendment of reports, automates

correspondence and tracking, securely redacts sensitive information and allows judges to file Periodic Transaction Reports. By supporting compliance with legal requirements, JEFS promotes transparency and accountability in the completion, submission, review, and release of financial disclosures reports. Additionally, the established public website facilitates online requests and releases of financial disclosure reports in accordance with the Courthouse Ethics and Transparency Act.

The JEFS roadmap includes evaluating the feasibility of migrating the system to a cloud-based infrastructure with the goal of enhancing system performance, security, and scalability, while ensuring alignment with broader technological advancements within the Judiciary.

Emergency Management Initiatives

Prominence of the judiciary in the news and social media sites has resulted in amplified negative public perceptions of the judiciary, increasing physical security risks to judiciary facilities, judges, and judiciary executives. The Judiciary remains committed to improving its ability to assess and mitigate security and emergency management-related risks to staff and facilities. The Judiciary does this through the Judiciary Security Vulnerability Management Program, which began in 2020. This program provides staffing and a suite of services to JSD to maintain a continuous monitoring process by which potential and actual judiciary physical security and emergency management programmatic weaknesses are identified, evaluated, prioritized, and mitigated.

The PII Reduction and Redaction Program conducts online exposure assessments and develops and implements personalized PII reduction strategies to mitigate online vulnerabilities of Judiciary protectees. This includes developing and providing individualized reports to judiciary protectees regarding the assessment of their current online exposure and associated risk, and the

mitigation strategies to be implemented by the AO's Facility and Security Office towards lowering their exposure and reducing their risk and qualifying any remaining risk at the end of each individual assessment and mitigation effort. These efforts include: 1) assessing and reporting on AO and Judiciary risks and vulnerabilities, both to judiciary protectees due to the presence of publicly accessible PII and AO and judiciary assets due to specific incidents (e.g., natural hazards, public health emergencies, first amendment related activities, etc.); 2) geospatial services utilizing spatial analytics to determine the relationship of emergent all-hazards incidents and other AO and Judiciary security and emergency management concerns to judiciary operations and assets; 3) training and developing skill and knowledge-based training and decision support tools for related topics (i.e., data privacy, geospatial services use, emergency notification services, etc.) for delivery (e.g., e-learning, classroom, blended) to judiciary protectees and family members, key judiciary staff, and partner agencies as appropriate; and 4) technical services coordinating within the AO to create and maintain a representative systems architecture, inclusive of Infrastructure as a Service, Software as a Service, and Platform as a Service environments, configurations, and data flows.

Through each component of the Judiciary Security Vulnerability Management Program Services initiative, the Judiciary continues to expand solutions to strengthen analysis of security and emergency management issues, communications, and situational awareness during emergency situations.

Judiciary Data Management and Governance

The Judiciary manages a broad array of information in its suite of national systems. As in many organizations, these systems were developed separately over time to support various lines of business, such as case management and court administration, probation and pretrial services, human

resources, and financial management. Although the systems were developed separately, the lines of business often share information in common, and their work processes are interconnected. As a result, the suite of systems stores redundant data and documents, and it can be difficult to share information and coordinate work processes across systems.

The Judiciary will further benefit both technically and programmatically by integrating its national systems and information. Eliminating multiple data repositories reduces data entry costs; it also eliminates the need to synchronize data across repositories, making data more consistent. The ability to share information easily and coordinate work processes across lines of business improves quality of service and increases productivity. Additionally, the availability of comprehensive and complete data across lines of business makes it possible to more effectively analyze organizational patterns and trends which, in turn, results in better planning and decision-making.

The Judiciary's efforts to manage data as an enterprise asset are guided by a data strategy and governance plan approved in 2021 with input from AO and court stakeholders. The plan, which is overseen by the AO Data Governance Board, identifies strategic principles, key activities, and measures of success for enterprise data, such as caseload, defender, finance, budget, human resources, probation and pretrial services, and space and facilities data. With input from the AO Data Governance Board, focus on achieving this vision over the last year has been on the following priorities. This version of the plan will be revised and updated as it has expired at the end of 2025.

Data Security: The Data Security Categorization Workbook was developed for use by court units, federal public defender organizations, and national program offices to strengthen the IT security posture of the Judiciary by ensuring data is categorized

consistently across the Judiciary's many systems. The AO implemented a web-based form to improve efficiency and automate the annual requirement to inventory information types held within the Judiciary's systems. The AO continued work to incorporate data classification into the data security program, which will be a long-term effort over the next several years. Data classification is focused on identifying sensitive information and marking or tagging it so that users of that information understand that it is sensitive, that there are safeguarding requirements, and that there are restrictions on its dissemination. A data classification schema will define the sensitivity of Judiciary data so that sensitivity-appropriate protection measures can be implemented.

Data Literacy: This is generally considered as "the ability to read, write and communicate data in context" or "speaking data." Increasing data literacy throughout the Judiciary is essential as technological advances allow for both creation and consumption of an ever-increasing amount of data. The AO launched access to resources to help Judiciary workforce members achieve the level of data literacy required for their roles. As part of the launch, the AO held a virtual data-focused conference for the Judiciary with sessions focused on data governance, artificial intelligence, and demonstrations of court and AO solutions leveraging data to make better decisions, drive efficiencies, and automate processes. The goal is to ensure that Judiciary users understand what the data represents and the source from which it comes, how it is or could be used, and who can distribute, access, and share the data.

Enterprise Data Management: As part of the CMM program, the AO is implementing enterprise case management data governance and stewardship, including developing data standards and policies to improve data quality and increase access to case management data.

The AO has continued implementing a data management tool to support self-service

analytics and better governed data. The tool supports increased transparency and access to data through the ability to trace data lineage and create a data catalog that clearly describes what the data is, where it is sourced from, and what can be done with it. With custom integrations in place that allow the tool to interact with enterprise reporting and transformation tools, the AO has focused on incorporating metadata (“data about data”) from the on-premises Enterprise Data Warehouse (EDW).

The AO continues to enhance the EDW platform by integrating additional functionality to better support tactical data and analytics needs. The AO is also embarking on modernizing IT and processes by acquiring and implementing cloud-based environment and data tools to gain functional, operational, and innovation efficiencies. PACTS360 program presented an opportunity to launch the Cloud Enterprise Data Warehouse (CEDW) to commence the modernization efforts.

Maximize National Systems through Court-Led Best Practices

Goals of the national IT program include developing and maintaining technology standards for all Judiciary IT systems—which empower local IT staff to develop solutions which integrate securely with national applications—as well as identifying common technology solutions to provide capabilities that reduce the proliferation of competing technology solutions. Nationally supported systems provide economies of scale, are critical to courts without the resources to develop their own systems, and provide some degree of standardization that allows courts, attorneys, and the public to share information more effectively. Additionally, the implementation of enterprise IT standards reduces technical complexities and subsequently reduces cybersecurity risks.

Although courts share the same general business processes, the specific ways they carry out those processes can vary widely. Many of these variations reflect local customs and preferences, as well as business needs, and are shaped by factors such as the type of cases that may predominate in a particular district, the size of the district, and the requirements of judicial discretion. To accommodate these variations, respond to a particular court’s business needs and priorities, and address requirements not met by national systems, the Judiciary’s national case management systems historically have allowed for individual court customization.

For the same reasons, courts also create adjunct systems, the requirements for which may be unique to an individual court or common to many courts. A priority of the national IT program is to facilitate sharing of local applications among courts and, where appropriate, make the functionality available nationally by incorporating those applications into national systems or by providing national support. For example, two calendaring applications² developed by local courts have been supported nationally for several years and are used by many judges and chambers staff. In addition, a local application called Citation Links, which was already being used by 17 courts (see [Judges and Chambers Staff](#), page 6), was added to NextGen CM/ECF. This model of incorporating valuable local developments into national systems will continue to be applied in the future. With NextGen CM/ECF going into ‘lights on mode’ there is an ask to the courts to stop making any more changes or creating new adjunct systems to work with NextGen CM/ECF. Evaluation of the adjunct systems and the problems they solve for the courts is in progress to determine if that should be subsumed into the CMM effort.

² Chambers Electronic Organizer (CEO) and Chambers Automation Program (CHAP).

Enterprise Strategy, Architecture and Innovation

Increasing Collaboration for Enterprise Strategic Growth:

The AO is expanding collaboration between business partners and IT stakeholders to ensure business requirements are being addressed effectively and efficiently. This allows the AO to clearly align goals with judiciary objectives and synchronize enterprise business priorities with the overall IT strategy. Collaboration fosters strong stakeholder engagement and enterprise strategic growth while ensuring the enterprise IT strategy meets the needs of the Judiciary.

Enterprise IT Standards: A structured lifecycle management process has been established for enterprise IT standards to promote Judiciary-wide technical standards and enhance interoperability. This process covers intake, development, publication, monitoring, and sunset of standards through structured collaboration with AO stakeholders, courts, and defender services. Standards requests submitted by senior leaders are triaged and objectively scored for priority, developed by subject matter experts, peer-reviewed, reviewed Judiciary-wide, and finally approved and published on the IT Standards SharePoint site and on JNet.

This framework strengthens the Judiciary's security posture, improves consistency and quality, reduces complexity, and supports IT modernization efforts. Compliance measurement and reporting will be implemented as supporting tools and metrics mature.

Innovation: A program will be developed to promote innovation in the Judiciary and to provide an approach to efficiently facilitate innovation ideas from throughout the Judiciary to the national level and eventually to implementation.

Network Enhancements

The Judiciary's public, private and virtual networks supporting all internal systems and enabling more widespread use of its public-facing technologies require that network capabilities be evaluated and upgraded on an ongoing basis. The Judiciary has completed the convergence of network services, delivering voice, data, and video services over a single, secure network. The converged network offers improved delivery of other services, including mobile computing, videoconferencing in the courtroom and elsewhere, delivery of distance training through collaborative technologies, integration of telecommunications with the Judiciary's software systems, and improved ability to support server centralization. The Judiciary has been realizing a stable and resilient network infrastructure from the implementation of a redundant data center core switching infrastructure. The completion of the Wide Area Network (WAN) Diversity project increased the overall network availability and reliability through carrier diversity and redundant connections.

National IT Operations

The Judiciary's National IT Operations delivers 24x7 frontline support for national judiciary IT services—combining customer service and operational insight to monitor, detect, and respond to service events—providing mission assurance while operating and maintaining secure networks, platforms, applications, and services. This supports all national services as the single operational interface point for IT customers, as well as, the infrastructure service provider to the courts.

Over the next year, the AO will consolidate several disparate national IT support operational functions and establish stronger centralized oversight of incidents and problem resolutions. The AO will expand enterprise-wide monitoring to reduce the frequency, duration, and business impact of IT service disruptions. Enhanced operational analytics and IT service management capabilities will

be integrated with existing tooling to improve visibility across all layers of the national IT environment.

Operations will leverage historical and real-time data to anticipate issues, drive timely corrective actions, and deliver clear, consistent communication to stakeholders.

Enhanced Hosting Services

Building upon the Judiciary's network is a robust platform of centralized hosting services that stands poised to fuel innovation across the organization. The Judiciary continues to implement and operate full enterprise, national-level hosting and private cloud computing services for courts and program offices, including infrastructure and other hardware, database storage, virtual applications, and server support. These services supply centralized and enhanced availability of Judiciary data and systems as well as an evolving catalog of public and private cloud-based solutions to the Judiciary. These solutions spur innovation, improve continuity of court operations and disaster recovery capabilities, and support a more mobile work force.

The design and implementation of a hybrid multi-cloud will integrate the current on-premises judiciary private cloud with modern and secure public cloud offerings. The acquisition of public cloud services will allow the Judiciary to provision modern cloud services to quickly meet individual business needs. This strategic move empowers courts to provision modern cloud services based on specific needs, utilizing a flexible, consumption-based funding model. The Judiciary's coordinated program will consider the potential cost, security, architectural and business impact, as well as other implications of cloud computing to provide guidance on these decisions. The overall benefit is increased operational flexibility, access to a continuously updated service catalog, and enhanced computing environment resiliency.

Backup modernization enhances the existing backup services by replacing aging tape backup technology and physical storage vaults with cloud storage for long-term data protection. Using cloud storage provides the Judiciary with faster mean time to recovery and perpetual retention without ever having to upgrade to newer format drives and tapes as the older tape technologies reach their end of support life. Modernizing backups with public cloud storage provides an online "hot" site for data in case one of the Internet Data Centers is offline due to disaster, further enhancing our disaster recovery capabilities in support of judiciary operations. Over the long term, leveraging public cloud storage for data retention opens possibilities for the Judiciary to apply advanced AI-driven analytics and data mining capabilities.

Courtroom Technologies

The Judiciary has made substantial investments in courtroom technologies (CT) that reduce trial time and litigation costs, improve fact-finding and juror understanding, and enhance public access to court proceedings. These capabilities include evidence presentation, videoconferencing, assisted listening, language interpretation, and electronic sound recording solutions.

Rapid evolution in the audiovisual industry continues to transform how technologies are implemented in courtrooms and courthouses. However, these advances also introduce maintenance challenges, as vendors frequently end support for legacy systems and ongoing supply chain constraints affect both sustainment and new installations. In response, the AO is executing a comprehensive modernization strategy grounded in a clear understanding of the current landscape and the use of standardized designs.

The AO is developing audiovisual over internet protocol (AVoIP) standards and designs for court of appeals, district, and bankruptcy courtrooms, as well as ancillary spaces. This work will establish updated

Judiciary-wide architectures, standards, and guidance that accommodate in-person, remote, and hybrid hearings.

The AO conducted a comprehensive courtroom technology Data Collection Effort to assess the current state of CT systems and identify modernization challenges across the courts. The resulting data will factor into CT allotment decisions and enable the AO to develop accurate estimates for future infrastructure funding needs. When combined with the AVoIP design project, industry benchmarks, and national design and integration contract cost estimates, this data will support robust predictive financial modeling and long-term strategic planning for courtroom technology modernization across all federal courts.

This coordinated, data-driven approach positions the Judiciary to efficiently modernize CT installations and infrastructure, reduce long-term operational and maintenance costs, strengthen cybersecurity posture, and ensure reliable, accessible, and future-ready support for judicial proceedings across the nation.

Communications

A Unified Communication and Collaboration (UCC) program originally launched in 2020 to streamline the collaboration and communication tools used by the Judiciary. Over the course of the program, multiple collaboration and communication solutions were evaluated and after initial assessment, some tools were discontinued or “sunset.” However, the analysis concluded that some of the telephone solutions did not have feature parities to allow further solutions to also be sunset. As technology has evolved and a lot has changed in how Judiciary employees work, the UCC space will be evaluated for opportunities to eliminate redundancy and optimize existing solutions with the objective of reducing costs and improving end-user experiences.

Artificial Intelligence

The Director of the Administrative Office (AO) established the Artificial Intelligence (AI) Task Force in 2025 to coordinate the policy issues that AI presents for the judicial branch and to recommend action by appropriate policy makers. Working in collaboration with judges, court staff, and judiciary stakeholders, the Task Force is conducting research, assessing risks and opportunities, and developing recommendations for policy and guidance to address the challenges presented by rapidly evolving AI applications. In line with Goal 5.1d of the *Strategic Plan for the Federal Judiciary*, the Task Force is currently developing a proposed AI governance framework to guide the responsible adoption and use of AI technologies across the federal judiciary and to manage risks and challenges presented by these new and evolving technologies. The proposed AI governance framework will address training, governance, procurement, IT security, and cost efficiency, among other areas, and is designed to support responsible adoption and deployment of AI in a manner consistent with judicial values.

AI initiatives will include implementation across applicable cloud platforms as well as exploratory efforts to understand how to leverage AI locally for productivity augmentation and increased automation.

Preventing Malicious Activity

Judiciary IT security responsibilities are shared by the national program, court units, and individual users. The national program promotes secure coding practices and architectural design, maintains a 24/7 security operations capability, provides security assessment and testing services, and conducts risk-based planning, among other activities. It also encourages court units to implement analogous concepts within their environments using network, system and data security techniques, security policies, access control and identity management practices, and related activities. Finally, it promotes an understanding of risk and a desire toward

end-user behavior that safeguards Judiciary assets and data.

The Judiciary implements a defense-in-depth strategy designed to protect networks, systems, and information through preventative and reactive measures. Network- and host-based capabilities are employed to routinely inspect traffic and devices for signs of malicious activity that can be blocked or identified for further analysis. Services, tools, and devices—such as firewalls at the boundaries between a court unit and the DCN as well as between the DCN and the internet—further prevent breaches. Identity and access management systems restrict access rights to Judiciary data, and web-based threat protection systems prevent end user access to known malicious sites on the internet. Finally, continuous diagnostics and mitigation identify vulnerabilities and anomalies for corrective action before they can be exploited. Over the next three to five years, the AO intends to focus its efforts within this category in the following areas:

Formal Assessments and Accreditation: The formal adoption of policy requiring the accreditation of National Program Office systems aligns the AO with best practices for risk-based assessments and management similar to the Executive Branch and the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). The cybersecurity accreditation and risk management program employs methodology from NIST Special Publication 800-53A for assessing controls, NIST Cybersecurity Framework (CSF) for AO security program management, and the Judiciary Information Security Framework (JISF) for systems security planning, development and accreditation. Over the course of the next five to seven years, the AO will focus efforts on assessing and accrediting new IT systems in development and accrediting current operational systems for all national programs.

Secure Coding Practices in Judiciary Applications: The AO has initiated efforts to

leverage development, security, and operations (DevSecOps) practices as a new approach towards application and system development in the federal Judiciary. By integrating security tools, automation, and assessments throughout the continuous integration and continuous delivery/deployment pipeline, the AO ensures that secure coding, testing, and mitigations are integrated into the lifecycle of new software and systems. Efforts will continue to adopt DevSecOps practices for all new AO modernization projects with the intent to expand to include court unit software and systems development.

Judiciary Vulnerability Management: Since 2021, the AO vulnerability management program leverages Department of Homeland Security Cybersecurity Infrastructure Security Agency Cyber Hygiene services, Commercial Bug Bounty services, and a public Vulnerability Disclosure Policy in addition to internal continuous diagnostics and mitigation (CDM) capabilities, and internal testing efforts to provide near real time visibility into the security posture of the Judiciary's assets and environment. Vulnerability detection and mitigation responsibilities at courts have been augmented by regional security teams at the circuit level and modernization of local endpoint security tools, providing better visibility of risks. Moving forward, the Judiciary plans to mature the organization's continuous diagnostic and mitigations (CDM) program to incorporate continuous asset discovery and validation, near-real time vulnerability detection, and improved automation and integration with a more feature-rich enterprise governance, risk, and compliance (GRC) platform to track vulnerabilities, findings, plans of action and milestones and risk acceptance.

National Logging Service (NLS): A centrally managed platform for collecting, retaining, searching, alerting, reporting, and analyzing large volumes of machine generated log and telemetry data in near real time, supporting courts, national program offices, and the Network and Security Operations Centers with

the visibility needed to identify, investigate, and resolve operational and security incidents across the national infrastructure. As usage continues to grow and observability demands increase, NLS is undergoing a strategic modernization upgrade of its hosting infrastructure to enhance performance, improve resiliency, and support higher ingestion volumes by consolidating log streams onto highly available collectors and optimizing computing and storage resources. These improvements will strengthen search performance, ensure more reliable data availability, and provide a scalable foundation closer to real time analytics. In parallel, the service is reducing its datacenter footprint through server consolidation and expanding its reporting catalog to address emerging operational and security use cases, ensuring that stakeholders across the Judiciary have timely, actionable insights to support mission critical decision making.

Judiciary Firewall Service (JFS): The Judiciary has installed dedicated security appliances to the boundary between each court and the DCN, reducing the likelihood that a malicious event will spread laterally among courts. Their placement ensures a consistent configuration across locations and complements the security infrastructure at the Judiciary data centers. The Judiciary has implemented additional capabilities to these firewalls, such as vulnerability protection, spyware, and antivirus blocks, and web filtering, which controls access to known hostile websites. As cloud and AI technologies have advanced, the JFS service has already begun to leverage its Security, Orchestration, Automation & Response (SOAR) capabilities. This more proactive threat management approach will be key within the next five years as initiatives like local area network (LAN) is implemented throughout the Judiciary. → Security policies will continually adjust to improve the security posture of each court location as well as the overall DCN.

Zero-trust Architecture (ZTA): The Judiciary is moving toward a zero-trust cybersecurity framework, meaning no user, device, or

system—inside or outside a network—is automatically trusted. Instead, ZTA requires continuous authentication, authorization, and validation before granting access to resources, using factors such as identity, device health, location, and behavior. Zero trust architecture enhances security by enforcing strict access controls and ongoing verification for every interaction. It is an overarching strategy that includes micro-segmentation, multifactor authentication (MFA), and identity, credential, and access management (ICAM).

The Judiciary is developing a roadmap to guide its zero trust adoption strategy. The roadmap will align with the Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model and National Institute of Standards and Technology (NIST) Special Publication 800-207 Zero Trust Architecture. It will serve as the Judiciary's strategic blueprint to evaluate our current Zero Trust maturity and establish a prioritized, risk-based path forward. By defining these specific Maturity Objectives, the Judiciary will create alignment across people, processes, and technology and transition from a perimeter-based defense model to one grounded in identity.

Micro-segmentation: Micro-segmentation is an essential function and a core principle of zero trust that will enhance the security of resources within the established isolated perimeters (identified under the identity, devices, data, network, and application workloads pillars of the ZTA model), allowing connections within each perimeter, but blocking access between them. This means that once a user or entity is authorized to access the network, they are limited to a specific, isolated space and resource, with limited ability to move laterally and access other systems. The Judiciary organization has initiated a strategy to implement micro-segmentation function as a single crucial metric with multiple modernization initiatives serving as factors to produce that metric. Notable modernization initiatives that contribute to producing the micro-segmentation function include, LAN

segmentation, Software-Defined Wide Area Network (SD-WAN), Secure Access Service Edge (SASE)/Cloud Virtual Private Network (Cloud VPN) solution, ICAM modernization, asset management modernization, data categorization, and application modernization. These initiatives will be worked through a phased approach that prioritizes segmentation of internet data center (IDC) resources first. Learnings from this phase will inform subsequent rollouts, ultimately encompassing all DCN resources. The phased approach ensures a smooth and efficient migration towards a higher zero trust maturity level.

Multi-Factor Authentication (MFA): As a core element of a zero trust, MFA is a security technology that requires two or more pieces of evidence (factors) to verify a user's identity before granting the user access to a network, system, or data. The Judiciary is advancing the national expansion and implementation of MFA as a foundational component of its ZTA strategy.

Initiatives focus on strengthening authentication capabilities by incorporating additional factors—such as hardware security keys and biometric passwordless authentication (e.g., facial recognition and fingerprints)—and extending MFA coverage to additional Judiciary applications and elevated-privilege access. To reduce user burden and support real-time risk assessment, the AO is exploring adaptive authentication and expanding the use of PIV-I credentials across systems, including VPN. These measures provide flexible, phishing-resistant authentication options tailored to diverse user communities while reducing reliance on passwords. The AO is further expanding MFA for external user authentication by leveraging standardized protocols and a government identity provider to support both authentication and identity verification.

Integrating these modern technologies strengthens protection against credential-based threats, streamlines user access, and facilitates secure access to systems and data.

This approach elevates the Judiciary's overall security posture, enhances usability, and ensures alignment with federal zero trust guidance. The MFA efforts are closely coordinated with the ongoing ICAM program.

Identity, Credential, and Access Management (ICAM):

The Judiciary is modernizing its Identity, Credential, and Access Management (ICAM) capabilities to strengthen assurance that the right individuals and services are granted the right access to the right resources at the right time. ICAM is a foundational component of the Judiciary's zero trust architecture because it shifts security decisions away from implicit trust based on network location and toward continuous verification of identity, device, session, and access context. Modernizing ICAM will enable the Judiciary to apply more consistent authentication, authorization, and access governance across national and local systems, whether users are accessing resources from within Judiciary facilities, remotely, or through cloud-based services.

Over the next three to five years, the Judiciary will continue implementing an enterprise ICAM approach that strengthens identity lifecycle management, expands use of phishing-resistant multi-factor authentication, improves federation and single sign-on capabilities, and supports more granular role- and attribute-based access decisions. These capabilities will enhance the Judiciary's ability to enforce least-privilege and just-in-time access principles. The Judiciary's ICAM modernization will also improve the visibility of user, service, and privileged access activity, supporting stronger governance, auditability, and risk-based decision-making across the enterprise.

ICAM modernization is closely tied to other infrastructure initiatives described in this plan. Identity-based policy enforcement is essential to the success of micro-segmentation, secure remote access, SASE/cloud VPN services, asset management, data categorization, and application modernization. As the Judiciary advances toward a higher level of zero trust

maturity, ICAM will serve as a unifying control plane that helps ensure access decisions are informed not only by who the user is, but also by device posture, resource sensitivity, session risk, and operational need. In this way, ICAM will help the Judiciary better protect sensitive information, limit lateral movement, and enable secure interoperability across modernized national systems, legacy applications, and hybrid cloud environments.

Asset Management: The Judiciary has established an initiative to address the need for an enterprise solution for asset management. Currently, technical solutions do exist within the Judiciary that support asset management business processes. However, these solutions are not comprehensive, and requirements exist related to various aspects of the asset management process that are not addressed by the current solutions. Further, the current solutions are not integrated and do not share any data. The goal is to create a solution that will reduce redundancy, realize cost savings, and enable efficient business processes without impacting court operations. The Judiciary is developing a comprehensive strategy to engineer and deliver the solution.

Security Infrastructure Modernization for Remote Access: After assessing existing remote access services, products, and infrastructure for opportunities to enhance and better secure the Judiciary's remote access program—particularly for providing DCN access to a variety of devices as well as improving the security, performance, and efficiency in remotely connecting to Judiciary resources—the Judiciary is implementing a cloud VPN service. The new cloud VPN will provide enhanced security and consistent access management for employees remotely accessing all Judiciary assets, irrespective of their location. Implementation of a cloud VPN supports the Judiciary's efforts to modernize its remote access infrastructure and support a zero-trust architecture.

Detecting, Analyzing, and Mitigating Intrusions

Activities in this area allow the Judiciary to act quickly and effectively in detecting and responding to security incidents. These activities include analyzing indicators of malicious activity, event notifications, remediation support, and digital forensics. Threat detection activities also include event correlation and analysis across multiple services, tools, and devices. These activities address the impact of intrusions on systems and applications, including incident response, log analysis and review, and actions to redress exploited vulnerabilities. Keeping these capabilities current requires continually evaluating cyber threat trends and their potential impact on Judiciary assets as well as incorporating data derived from new tools and sources. Priority efforts in this area will include the following:

Enhanced Endpoint Security: Combining Endpoint Detection and Response capabilities in addition to the Judiciary Endpoint Security Suite of tools allows the AO to rapidly assess and take action on any devices that may be compromised or at risk, to preserve evidence, contain hackers and hacker tools, and prevent further intrusion. Efforts to enable network based forensic endpoint triage have successfully deployed across critical systems and networks, with additional capacity deploying across the enterprise over the next two to three years.

Hunt Team Service: To identify any potential cyber-adversaries deeply embedded within the Judiciary network, a specialized team of security professionals proactively and systematically searches for evidence of known cyber-criminal tools, tactics, and techniques. This team also investigates abnormal user and machine behavior. Hunt operations are pivotal in adding context to, and expanding, the scope of investigations across the enterprise.

Shaping the Cybersecurity Environment

The Judiciary creates and maintains a security-aware culture using recognized best practices for information security. Development and oversight of the *Judiciary Information Security Framework* (Framework) provides the foundation to effectively manage risks, make informed decisions about implementing safeguards, and continually assess safeguards for suitability and effectiveness. Policies, tools, and other resources facilitate implementation of Framework concepts across the Judiciary. As IT security is a shared responsibility, court units and federal public defender organizations (FPDOs) need policies, tools, information, and education to perform their role. Over the next three to five years, the AO intends to focus its efforts in this category in the following areas:

IT Security Education: The IT security training curriculum continues to expand and evolve to meet the ever-changing IT security needs of the Judiciary. The program, launched in 2017, includes course offerings which provide court and FPDO IT security professionals with the knowledge required to pursue nationally recognized cybersecurity certifications while at the same time delivering in-depth training on the security tools utilized by the Judiciary. Training offerings continue to raise the level of cybersecurity knowledge and skills in the Judiciary. In 2023, the Judiciary implemented a policy making two baseline cybersecurity courses mandatory for all IT professionals. The policy also requires 40 hours of continuing education training every two years. As the cybersecurity landscape changes, new training curriculums will be offered, enabling IT security professionals to acquire the skills necessary for the Judiciary to stay abreast of IT security needs.

Cyber Threat Intelligence: Open-source intelligence collection and analysis

strengthens the national IT security program by identifying new vulnerabilities, detecting imminent threats, identifying attack trends, using global commercial and government metrics, and coordinating with external partners in law enforcement, other government agencies, and non-government organizations to act on credible indicators of harm. Intelligence analysts enhance situational awareness and provide threat attribution to bring context to threats targeting the Judiciary. The AO has fully integrated with the National Cyber Intelligence Joint Task Force and continues to build capacity in integrating with the Intelligence Community and Executive Branch partners.

Investing in the IT Program

The Judiciary aligns its IT investments with its business objectives through an inclusive planning process that is synchronized with the Judiciary's budget cycle. The Judicial Conference Committee on Information Technology reviews resource requirements and expenditure plans for the Judiciary's IT program in accordance with guidelines and priorities established by the Judicial Conference for the use of available resources.

When considering the costs associated with the IT program, it is important to take a broad Judiciary-wide view. The Judiciary's public-facing technologies, internal systems, technical infrastructure, and security program have resulted in improved central services to its external stakeholders as well as internal efficiencies that have allowed the courts to absorb an increased workload without increasing staff as much as would otherwise have been required. These cost avoidances have become increasingly important in times of continuing budgetary constraints.

The Judiciary will continue to rely heavily on its IT program to meet its mission and to serve the public in the coming years. As indicated in this annual update to the *Long Range Plan*, not only will existing systems and

infrastructure be maintained and enhanced, but it is critical that emphasis be placed on investing in new systems, technologies, and services that will modernize the Judiciary's IT infrastructure and provide additional benefits, including the protection of assets from cyberattacks.

The table below shows the Judiciary's anticipated IT resource requests for FYs 2027 through 2031, organized by category within the Judiciary Information Technology Fund (JITF).³ Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

Resource Requirements

JITF Program Component	Current Estimate (Dollars in Millions)				
	FY 2027	FY 2028	FY 2029	FY 2030	FY 2031
Administrative and Mgt Systems	100.6	115.5	194.6	197.5	197.0
Court Administration and Case Mgt	52.2	211.4	101.4	92.6	86.8
Court Allotments	135.3	133.4	138.0	140.2	143.1
Court Support	115.6	135.9	138.7	141.4	145.4
Cybersecurity & IT Modernization Plan	49.7	0.0	0.0	0.0	0.0
Infrastructure and Collaboration Tools	216.6	204.4	258.5	277.3	263.0
Judicial Statistics and Reporting	18.5	17.4	18.3	18.0	19.1
Telecommunications	122.3	154.9	150.1	158.7	188.1
<i>Subtotal</i>	810.7	972.9	999.6	1,025.7	1,042.5
Electronic Public Access Program	233.8	307.1	298.5	253.8	240.5
<i>Total JITF Financial Requirements</i>	1,044.6	1,280.0	1,298.1	1,279.5	1,283.0

³ Section 612 of Title 28, United States Code, establishes the JITF and makes funds available to the Judiciary's information technology program without fiscal year limitation.

JITF Program Components

Administrative and Management Systems

This program includes the Judiciary's financial and personnel management systems, as well as systems to support and manage space and facilities projects, travel expenses, and Judiciary websites.

Court Administration and Case Management

This category contains a variety of tools, including the probation and pretrial services case management system; to access critical case information and law enforcement databases; systems for juror qualification, management, and payment; tools for jury participants to communicate with the courts; as well as the system that captures requests for payments to private court-appointed counsel and expert service providers.

Court Allotments

These funds are allotted to the courts to pay directly for operating, maintaining, and replacing computers, printers, local-area-network equipment, and software as well as local telecommunications services, equipment, maintenance, and courtroom technology.

Court Support

Court support funds AO staff that provide IT development, management, and maintenance services to the courts. These services include IT policy and planning guidance; architecture and infrastructure support; courtroom technologies; security services; development, testing, and implementation of national IT applications; IT training; and other administrative and IT support services on behalf of the courts.

Cybersecurity & IT Modernization Plan

This category encompasses requirements related to the Judiciary's multi-year cybersecurity and IT modernization plan. These funds will be dedicated to high-priority cybersecurity efforts and modernizing aging legacy systems or applications that are based on vulnerable programming technologies or technologies that are becoming obsolete.

Infrastructure and Collaboration Tools

This category encompasses building and maintaining a robust, reliable, and resilient Judiciary-wide IT infrastructure. Included are the costs of hardware, software, and IT security associated with the Judiciary's full enterprise hosting and cloud computing services and email and collaboration systems. It also includes the costs of IT infrastructure for new courthouse construction projects and operating systems support, maintenance, testing, security, and research.

Judicial Statistics and Reporting

This category includes systems to support gathering and reporting statistics in the Judiciary; data analysis and management reporting across Judiciary-wide data sources, and planning and decision-making with staffing, financial, and workload data.

Telecommunications

This category includes support for voice and data transmission services and telecommunications. The Judiciary's communications program enables the Judiciary to operate communications services for the appellate, district, and bankruptcy courts as well as probation and pretrial services offices. It also enables the Judiciary to procure communications equipment for new courthouses and for courthouses undergoing major repairs and alterations.

Electronic Public Access Program

This category provides electronic public access to court information; develops and maintains electronic public access systems such as CM/ECF in the Judiciary; and provides centralized billing, registration, and technical support services for the Judiciary and the public through the PACER Service Center.



Administrative Office of the United States Courts
Washington, D.C. 20544

www.USCourts.gov