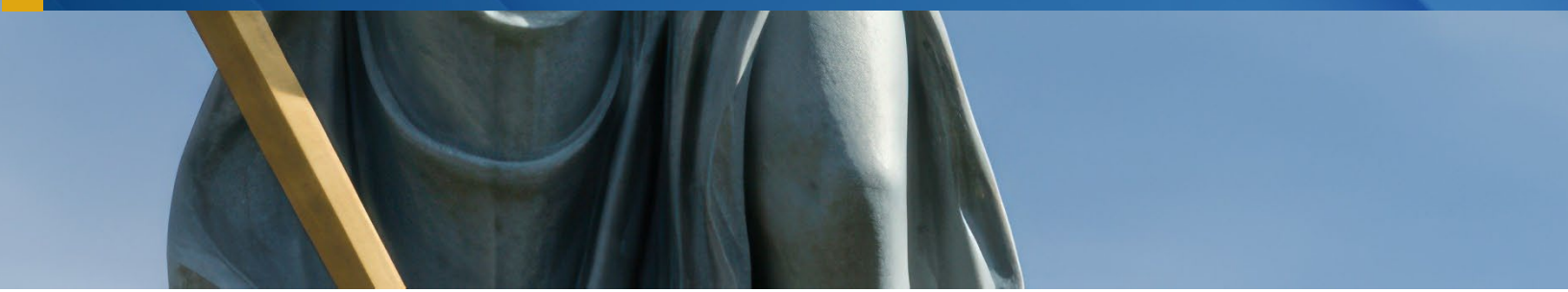
Administrative Office
of the United States Courts

Long Range Plan for Information Technology in the Federal Judiciary

Fiscal Year 2026 Update

10/01/2025



Long Range Plan for Information Technology in the Federal Judiciary: Fiscal Year 2026 Update

Table of Contents

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) 2026 through FY 2030. The strategic priorities discussed in this document integrate the *Strategic Plan for the Federal Judiciary*, as updated in 2020, 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 four 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 2020.

Strategic Priorities

The *Strategic Plan for the Federal Judiciary* combines the strategy of, "Harnessing the potential of technology to identify and meet the needs of court users and the public for information service, and access to the courts," 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 four associated goals which form the basis of the strategic priorities for IT:

- Continue to build, maintain, and continuously 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, case management, and administrative support.
- Coordinate and integrate national IT systems and applications from a Judiciary-wide perspective; continue to utilize local initiatives to improve services; and leverage Judiciary data to facilitate decision-making.
- Develop system-wide approaches to the utilization of technology to achieve enhanced performance and cost savings.
- Continuously improve security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information. In addition, raise awareness of the threat of cyberattacks and improve defenses to secure the integrity of Judiciary IT systems.

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

Strategic Priority
Continue to build, maintain, and continuously 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, case management, and administrative support.

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.

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 4.6 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 described below. The CMM effort will deliver a modern, sustainable digital platform for the Judiciary to manage cases, provide public access to court records, and improve communication, collaboration, and engagement among courts and the public.

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 PACER.gov.

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. They have

participated in regular user research sessions that will focus on requirements for various features of the new system as the project has advanced through the development lifecycle.

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; enhances the Judiciary's ability to exchange data within its internal and external systems; supports a more consistent user experience for external users; improves filing capabilities for pro se filers in bankruptcy cases; and provides 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 support the work on the CMM effort which will replace NextGen CM/ECF.

The AO started the CMM effort in March 2022 to develop a modern, sustainable platform for the Judiciary to manage cases and improve communication, collaboration, and engagement among courts, the public, and other partners. Part of the CMM effort includes adding "unified 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.

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, uses Software as a Service (SaaS), which is a highly configurable Microsoft platform-based solution. In November 2023, the AO announced that there will be a delay in the completion and the rollout planned for FY 2024. After detailed analysis and with corrective measures implemented, the development has progressed and is currently close to wrapping up in FY 2025 with the rollout to the pilot districts scheduled for the

second quarter of FY 2026. The replacement system will continue to interface with key applications, both internal and external to the Judiciary, and provide officers the data necessary to fulfill their mission. Replacement is a multi-year project, with work completed in stages. Operations and maintenance, including cybersecurity of the application, will begin with the initial rollout in FY 2026 and incrementally grow in the number of licenses required through FY 2027. The program office is planning to issue additional call orders in 2027 for the development of program management and advanced data analytics capabilities to support the mission of the probation and pretrial services offices.

eVoucher and Vendor Manager (Criminal Justice Act (CJA) products): CMSO is responsible for the development, operations, and maintenance of the CJA eVoucher product, 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 also 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 February 2025, we released the vendor manager application to the district court of Oregon as part of a pilot release. This was highly successful following which the new, integrated vendor management application was rolled out to all district courts in March 2025. The national rollout was highly successful as well. The new vendor manager application provides a modern, web-based application that enables invited Judiciary vendors to manage their contact, tax certification, and bank account information. The vendor manager module is fully integrated with eVoucher and JIFMS, increasing vendor satisfaction and improving compliance by enabling CJA payments to be sent via electronic fund transfers (EFTs) which helps the Judiciary comply with the treasury and IRS requirements. As part of the eVoucher modernization effort an assessment was done to understand what it would take to migrate the eVoucher and Vendor Manager applications to a Judiciary-approved cloud service provider (CSP). The team is now working on human centered design to define the scope of the minimum viable product that they will develop to replace eVoucher incrementally.

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 has been using the same client/server-based jury management system for over 20 years, with the current contract set to expire in 2027. The current 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) the vehicle for prospective jurors to submit a statutorily required 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. A contract will be awarded for a web-based solution that is expected to be more cost-efficient and easier to support. The web-based solution 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. The AO plans to roll out a modified commercial off-the-shelf system that will meet court needs.

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 resources (e.g., LexisNexis, Westlaw). 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.

Modernizing JIFMS was a critical foundational upgrade to the current version of the commercial off the shelf (COTS) solution, which implemented in FY 2025. This upgrade improved system security, provided support for the latest infrastructure, and positioned the Judiciary to begin introducing operational efficiencies and enhancements. These improvements include integrations and interfaces that promote financial management best practices. Updating the system enables improved integrations with budget, acquisitions, internal controls, and financial systems with government-wide solutions, such as the Invoice Processing Platform (IPP), G-Invoicing, and travel management to align with statutory and regulatory changes. 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 will continue with the "back to baseline" strategy, which minimizes Judiciary-specific customization of the underlying COTS 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): As of December 2023, the AO has fully implemented ACR, which replaces various cash register systems used by district, bankruptcy, appellate, and national jurisdiction courts. This implementation moved the Judiciary to an enterprise platform that leverages modern software and infrastructure. The solution also integrates

with the Judiciary's financial and case management systems. With the court community using a single system, the Judiciary is well positioned to meet future legislative, business, and technological requirements. The AO continues to explore opportunities to enhance ACR's capabilities with other systems that will reduce data entry and improve operational efficiencies.

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 enhance the system 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 assessing the feasibility of migrating HRMIS to a cloud-based infrastructure. This effort aims to enhance system performance, security, and scalability, while aligning with broader technological advancements within the Judiciary. This effort will require careful evaluation of investment needs and business functionality trade-offs to ensure seamless operational continuity.

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 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. JEFS 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: The Judiciary is committed to improving its ability to assess and mitigate security and emergency management-related risks to staff and facilities. The Judiciary mitigates these risks through the Judiciary Security Vulnerability Management Program Services[2] initiative, which began in 2020. This initiative provides the Judiciary with increased situational awareness before, during, and after incidents, improved data privacy and vulnerability management in accordance with the Daniel Anderl Judicial Security and Privacy Act[3], and a new emergency notification system.

Situational awareness during an emergency incident is crucial for helping the Judiciary make informed decisions, anticipate risks, and respond effectively, which can save lives and minimize damage. The improved situational awareness program leverages a geospatial tool that provides the Judiciary with the capability to visualize, analyze, and disseminate information on hazards that have the potential to impact operations, or are currently impacting operations. Such hazards include, but are not limited to, natural disasters, public health emergencies, transportation incidents, preparedness issues, Judiciary security projects, security issues, and other threats.

The Data Privacy and Vulnerability Management program provides the Judiciary with a full suite of Personally Identifiable Information (PII) redaction and legislative support services in accordance with the Daniel Anderl Judicial Security and Privacy Act. The Judiciary's Data Privacy and Vulnerability Management efforts provide the full scope of Anderl Act data privacy and vulnerability management activities, protecting the Judiciary, and supporting over 2,300 federal judges and their immediate families with critical life-safety and security applications. This is achieved with a combination of geospatial, analytical, and data privacy

[2] The Judiciary Vulnerability Management Information Services was previously called the Judiciary Disaster and Recovery Tool (JDART).

[3] The Daniel Anderl Judicial Security and Privacy Act was passed in December 2022. It empowers the AO to support monitoring the internet for Personally Identifiable Information and other data elements that can put judges and their families at risk (covered information), removing covered information, coordinate vulnerability management activities with relevant public safety and security agencies, and report any judicial threats found during Judiciary implementation of the Act to the U.S. Marshals Service (USMS).

software services and infrastructure-as-a-service secure platforms.

The Judiciary is advancing its emergency management initiatives by conducting a national rollout of a new emergency notification system, which enables rapid and widespread dissemination of critical information, allowing for timely responses which can save lives and minimize damage in an emergency. This secure, stand-alone platform is a commercial off the shelf product that has been configured to meet the needs of the Judiciary. The new solution builds upon the functionality of the current emergency notification system by increasing message capacity, improving two-way communication, facilitating information sharing with federal agencies and partners, and expanding the reach and access of critical communications.

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.

Strategic Priority
Coordinate and integrate national IT systems and applications from a Judiciary-wide perspective; continue to utilize local initiatives to improve services; and leverage Judiciary data to facilitate decision-making.

Coordinate and Integrate National IT Systems and Applications

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.

These inefficiencies are being addressed, in part, through emphasis on technical standards, which will establish a framework to align investments with business and technology priorities and increase interoperability among technical solutions. The Judiciary's technical standards management process provides a structured and transparent approach to develop, review, and adopt technical standards, including feedback from Judiciary stakeholders.

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:

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 defined by Gartner[4] 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.

[4] Gartner is a leading research and advisory company. More information is available at https://www.gartner.com/en/about.

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 applications[5] 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 section, page 5), 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.

To promote Judiciary-wide technical and operational standards and enhance interoperability, a new lifecycle management process has been developed for all enterprise IT standards. The process for managing the lifecycle of enterprise IT standards will be facilitated by the AO but consists of an inclusive and transparent development approach involving representatives from both the AO and the court communities. The adoption of enterprise IT standards will be mandatory for all national and local systems, and compliance with the new standards will be regularly measured and reported against. In addition, a catalog of national applications is in development and will be extended to include locally developed applications to identify duplication of efforts, encourage collaboration, highlight gaps in the functionality of national applications, and promote communities of practice and technology knowledge-sharing. Finally, an innovation program will be developed to

[5] Chambers Electronic Organizer (CEO) and Chambers Automation Program (CHAP).

promote innovation in the Judiciary and to provide a framework to efficiently graduate innovation ideas from the local to the national level and eventually to implementation.

Strategic Priority
Develop system-wide approaches to the utilization of technology to achieve enhanced performance and cost savings.

The Judiciary continues to seek productivity enhancements and cost avoidance from new or improved IT systems, which provide efficiencies and help contain growth in future technology and staffing costs. Moreover, investments that reduce the complexity of IT systems also have the potential to produce savings and cost avoidances. The Judiciary's reliance on IT means that failure of its technical infrastructure can effectively bring operations to a halt for its internal stakeholders and severely affect the work of its external stakeholders. Therefore, reducing the complexity of the infrastructure and building a reliable national infrastructure that minimizes downtime, rework, and inefficiencies have been and remain objectives of the Judiciary's IT program. Areas on which the Judiciary will place especially high priority over the next three to five years are described below.

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.

Increase in cyber threats from adversaries has heightened the need to strengthen our network services security posture. The Judiciary is now focused on leveraging the Zero Trust Architecture (ZTA) principles to identify components connected to the Judiciary network, establish trusted zones for these components, and securely communicate with other components that reside within or outside the established trusted zones. The Judiciary is adopting an approach that leverages Zero Trust Maturity Model (ZTMM) to implement ZTA principles. Local Area Network (LAN) segmentation and Software-Defined Wide Area Network (SD-WAN) modernization initiatives based on ZTMM, are aimed at continuously enhancing network visibility, enforcing encrypted traffic flows internally and externally, and integrating dynamic, identity-aware access controls to ensure network access is granted on a least-privilege, session-by-session basis.

Our long-term network strategy centers on progressively implementing finer-grained segmentation (micro-segmentation) to isolate workloads and limit lateral movement, effectively treating all network locations as untrusted.

In addition to establishing trusted network zones, a Secure Access Service Edge (SASE)/Cloud Virtual Private Network (Cloud VPN) solution implementation has also been initiated to monitor and proactively prevent unauthorized access to the Judiciary's network.

Enterprise Operations Center

The Judiciary's Enterprise Operations Center (EOC) provides 24/7/365 monitoring of the national infrastructure, services, and applications to proactively identify IT issues before they impact end users, provide centralized event coordination, and decentralized situational awareness. The EOC supports all national infrastructure and applications and serves as the single IT service desk and court interface for incidents related to national infrastructure and applications.

Over the next few years, the EOC will consolidate several disparate national IT support functions and provide improved centralized oversight of incidents and problem resolutions. The EOC will provide increased user support to monitor the national infrastructure and applications to reduce the frequency and duration of outages. New operational analyses and IT service management tools will be coupled with existing tools to increase and enhance operational visibility into all layers of the national IT infrastructure. Historical and real-time data will be used to forecast potential problems, take corrective actions, and provide clear communications to all 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 full enterprise, national-level hosting and private cloud computing services for courts, 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 private cloud-based solutions to the courts. 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 readily available 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 quickly 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 will be to increase operational flexibility, cost efficiency, and resilience of the computing environment.

Backup modernization enhances the existing Hosting Service Backups by replacing aging tape backup technology and physical storage vaults with Public Cloud Service Provider storage for long-term data protection. Using public 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. On an even longer timeline, using public cloud storage for long-term data retention opens possibilities for the Judiciary to use AI data mining tools.

Courtroom Technologies

The Judiciary has made substantial investments in courtroom technologies that reduce trial time and litigation costs, as well as improve fact-finding, understanding by the jury, and access to court proceedings.

Rapid changes in the audiovisual industry have changed the way technologies are implemented within the courtroom and courthouse, but also present maintenance challenges, as suppliers regularly transition support to newer technologies. and current supply chain issues are also impacting maintenance and new courtroom technology installations.

The AO is surveying the current courtroom technology set up across the country, which will be the basis for the development of Judiciary-wide architectures, standards, and designs for CT to facilitate the efficiency of trials and hearings. The artifacts will identify an integrated set of technologies and capabilities that will accommodate in-person, remote and/or hybrid hearings, and account for factors such as AV equipment on the network, physical and cybersecurity requirements and monitoring, cloud-based and artificial intelligence solutions, and human factors such as the Americans with Disabilities Act and public access to proceedings.

Communications

The AO transitioned Judiciary users from AT&T Audio Conferencing service to Cisco Webex by November 30, 2024. This change came after thoroughly reviewing all toll-free service options as mentioned in a March 13, 2023, memorandum. Consolidating the toll-free service capability to one solution helps streamline the Judiciary's conferencing and unified communications solutions to ensure we fulfill court business needs while eliminating duplicative services.

SharePoint Online (SPO) is the main collaboration and document management tool within Microsoft's Office 365 platform. It includes functionality to collaborate, share, and store information across the Judiciary in a way that was previously not possible. The AO began a waved Judiciary-wide SPO implementation which was scheduled to be completed in July 2021 with 310 court units and the AO onboarded. As of March 2025, there remain approximately 21 court units that are working to complete SPO onboarding and 11 that have yet to begin the process. The inaugural Judiciary SharePoint Online Conference was held virtually in October 2024, with more than 800 individual Judiciary staff in attendance over three days to hear court staff share how they benefit from SharePoint solutions. It was a huge success. The JDAO plans to continue to offer the conference bi-annually. In November 2024, the Catalog of SPO sites and Microsoft Teams available to everyone in the Judiciary was published and provides a central list of sites and teams supporting cross-court initiatives. A catalog like this, where court users can browse for available Judiciary-wide resources, was not currently available. It is a welcome addition to the SharePoint resources available from the SharePoint Online Center of Excellence (SPOCOE) website.

The focus in 2025 is enable and empower onboarded courts to leverage SharePoint and related tools to design, develop, and deploy solutions that improve communication and collaboration and increase business process efficiency. The SPOCOE website, which serves as the hub of SPO information in the Judiciary, will continue to provide news and events, access to the archive of the Office Hours series of weekly webinars, Judiciary use cases, curated links to training, SPO governance, along with tips, tricks, and best practices. When requested, the team will continue to present at Judiciary conferences to share SharePoint success stories, promote SharePoint education and capabilities, and improve SharePoint adoption. Ongoing tailored support will be available to the Judiciary through the popular SharePoint Sherpa and SharePoint Skill Builder services.

Strategic Priority
Continuously improve security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information. In addition, raise awareness of the threat of cyberattacks and improve defenses to secure the integrity of Judiciary IT systems.

The national IT security program protects Judiciary information systems, services, and data against disclosure, unauthorized use, modification, damage, inaccessibility, and loss. In collaboration with the court community, this program fosters a security-aware culture and promotes support for initiatives that preserve the confidentiality, integrity, and availability of information associated with all forms of technology used by the Judiciary. The program provides the Judiciary with the information needed to make informed, risk-based decisions essential to safeguarding the deliberative process.

Technology introduces security risks that need to be managed on an ongoing basis, and the Judiciary faces the challenge of balancing the benefits of these technologies with those risks. The internet, as well as the Judiciary's IT environments, its underlying infrastructure, the applications that serve its mission, and the people who interact with these systems, are vulnerable to a wide range of cyber threats and hazards. In part, sophisticated attackers aim to exploit vulnerabilities to disrupt operations, gain access to sensitive court work products for financial or political gain, or to damage the reputation of the Judiciary and the nation, and are continuously developing new capabilities to disrupt, degrade, or deny the delivery of essential services. Addressing these threats requires the use of multiple measures in the following areas: 1) preventing malicious activities; 2) detecting, analyzing, and mitigating cybersecurity intrusions; and 3) shaping the cybersecurity environment.

Underpinning each of these is a tiered security architecture that separates resources based on data, business criticality, and function. Robust planning provides for continuous evaluation and improvements to adapt to the ever-changing threat environment and helps ensure that resources are focused where they provide the most benefit. The resulting data is analyzed to determine areas of vulnerability; to identify and respond to attack patterns and trends; and to update and continuously improve policies, procedures, and technologies commensurate with risk.

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.

Preventing Malicious Activity

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 (both network and web application) at the boundaries between a court unit and the data communications network (DCN) as well as between the DCN and the internet—further prevent breaches (as do network access controls, endpoint protection systems,

encryption solutions, patch management solutions, and multi-factor authentication). 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 security testing and assessments proactively identify vulnerabilities for corrective action before they can be exploited. Over the next three to five years, the AO intends to focus its efforts in this category in the following areas:

Formal Assessments and Evaluations: The cybersecurity assessment program employs a risk-based approach that evaluates the strength and resilience of court unit and AO national program office systems against potential threats and vulnerabilities. Results from these assessments inform the development and implementation security strategies and initiatives to enhance the Judiciary's overall cybersecurity posture. As a result, ITSO will expand and accelerate its accreditation program which assesses, authorizes, and continuously monitors the security of information systems throughout its lifecycle.

Secure Coding Practices in Judiciary Applications: In 2022, and consistent with industry best practices, the AO initiated efforts to leverage 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: Starting in 2021, the AO developed a coordinated vulnerability management program leveraging Department of Homeland Security Cybersecurity Infrastructure Security Agency Cyber Hygiene services, Commercial Bug Bounty services, and a public Vulnerability Disclosure Policy. The integrated vulnerability management program receives scan results and testing discoveries through a single intake and validation system that triages and prioritizes findings for courts and AO program offices to action and remediate. 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 court utilization of the enterprise governance, risk, and compliance (GRC) platform to track vulnerabilities, findings, plans of action and milestones and risk acceptance.

Blue Team Service: Blue Teams provide subject matter expertise to assist court units and program offices with developing plans of action to address discovered vulnerabilities and risks and provide technical assistance with implementation as necessary. Moving forward, AO Blue Teams will increase availability of services to courts and program offices to assist local system owners and ISOs with hardening systems, documenting security controls, and developing local cyber workforce talent to holistically improve Judiciary cybersecurity programs at the enterprise and local levels.

National Logging Service: A centrally managed platform that enables courts and national program offices to collect, retain, search, alert, report, and analyze large volumes of computer-generated log data in near real-time. This service is designed to help identify and troubleshoot IT incidents—both general and security-related—across the national infrastructure. By providing powerful log analysis capabilities, it empowers users to detect and resolve issues before they escalate. With comprehensive searching, dashboarding, and alerting features, the

platform ensures timely responses to potential threats and system abnormalities. The architecture is built to scale and adapt to the evolving needs of its users, offering an effective solution for log management across the Judiciary. In 2025, the focus will center on increasing resilience for streamed data by consolidating log feeds to highly available collectors. Additionally, we will be consolidating a large number of servers to reduce the datacenter footprint. The AO is also expanding its report catalog to include additional coverage for emerging security use cases.

Judiciary Firewall Service: The Judiciary has installed dedicated security appliances (Nextgen firewalls) 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 URL filtering, which controls access to known hostile websites. As courts become more proficient in identifying threats and risks, security policies are continually adjusted to improve the security posture of each location as well as the overall DCN.

Zero-trust Architecture (ZTA): The Judiciary is moving toward a zero-trust architecture, an information security model that is focused on the elimination of implied trust throughout the Judiciary's infrastructure and requires verification for every user, device, and application attempting to access an organization's network resources, regardless of device type or ownership (e.g., Judiciary furnished, personally owned, or other devices such as a hotel kiosk). ZTA limits access to network resources to only those authorized.

Micro-segmentation: Micro-segmentation is an essential function and a core principle of zero trust solution 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 producing the micro-segmentation function include, Local Area Network (LAN) segmentation, Software-Defined Wide Area Network (SD-WAN), Secure Access Service Edge (SASE)/Cloud Virtual Private Network (Cloud VPN) solution, Identity Credential and Access Management (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): Another element of a zero-trust architecture, 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 pursuing national expansion and implementation of MFA. Most recently, the Judiciary has launched MFA for PACER users. PACER users with filing or other CM/ECF-level access will be required to use MFA by the end of calendar year 2025. All other PACER users

will have the option to use MFA, but it will not be required.

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 pursuing implementation of a cloud VPN service. Upon implementation, a 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 react quickly and effectively to suspected security incidents. These activities include analyzing indicators of malicious activity detected by the mechanisms previously described, including event notifications, remediation support, and data forensics. They also include event correlation and analysis of activities across multiple services, tools, and devices. These activities address the impact of intrusions on systems and applications, including incident response plans, 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. Priority efforts in this area will include the following:

Log Management, Analysis, and Notification: Introduction of additional security capabilities and logging from the mandatory adoption of enterprise security tools and configurations has created a significant increase in the volume of logs the AO must analyze for threat indicators. Proper and timely utilization of aggregated logs require improvements to logging configuration and management to obtain relevant and useful data suitable for analysis with machine learning and other advanced techniques.

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 are underway to mitigate the risks of personally owned devices.

Red Team Service: Using tactics commonly employed by malicious actors and adversaries, Red Team services validate network defenses by identifying vulnerabilities to inform and enable continuous improvement. The existing Red Team personnel currently alternate between discrete iterations of a continuous exercise against the AO's infrastructure and fulfilling court requests for stand-alone adversary-emulation exercises. Planned expansion of the program will increase both the number of

courts that can benefit from this service, and the frequency of iterations in the exercise against the AO.

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 also entered into a formal relationship with the National Cyber Investigative Joint Task Force (NCIJTF) to provide liaisons on their operational watch floor. This arrangement grants the Judiciary access to classified databases, lines of communication, and daily briefings from intel analysts, communications specialists, technical experts, and other Intelligence Community agencies. Additionally, the AO is receiving quarterly classified briefings from the Cybersecurity and Infrastructure Security Agency (CISA), an agency within the Department of Homeland Security (DHS), on classified cybersecurity topics related to the Judiciary. Efforts are underway to gain additional access to consistent classified data and to monitor for threats targeting the Judiciary.

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. However, the Judiciary has substantial amounts of equipment at "end of life" and "end of service" across the Judiciary. This reality introduces operational and security risk, inhibits investment in modern technologies like the cloud, and results in overall service reductions to the court community. 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 2026 through 2030, organized by category within the Judiciary Information Technology Fund (JITF).[6] Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

[6] 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.

Resource Requirements

	Current Estimate (Dollars in Millions)				
JITF Program Component	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
Administrative and Mgt Systems	83.3	100.6	173.4	185.9	184.0
Court Administration and Case Mgt	26.4	47.7	85.1	65.2	60.2
Court Allotments	130.9	135.3	136.0	138.0	140.1
Court Support	115.5	117.8	136.1	139.4	141.9
Cybersecurity & IT Modernization Plan	72.3	49.7	0.0	0.0	0.0
Infrastructure and Collaboration Tools	206.6	218.8	235.1	233.6	234.0
Judicial Statistics and Reporting	17.5	20.7	15.7	16.7	17.5
Telecommunications	125.5	122.3	160.3	139.8	138.1
Subtotal	778.0	812.9	941.7	918.6	915.8
Electronic Public Access Program	231.0	228.3	235.3	238.7	220.5
Total JITF Financial Requirements	*1,009.0*	*1,041.2*	*1,177.0*	*1,157.3*	*1,136.3*

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