Fiscal Year 2024 Update

Long Range Plan for Information Technology in the Federal Judiciary

Long Range Plan for Information Technology in the Federal Judiciary: Fiscal Year 2024 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 a means to perform their jobs. As business processes and technology solutions have become interwoven, the Judiciary recognizes that IT plays a significant role in the work of the Judiciary and offers opportunities to develop more efficient and effective processes supporting successful outcomes.

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) 2024 through FY 2028. 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 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.

---

[1] Strategic Plan for the Federal Judiciary, approved by the Judicial Conference of the United States, September 2020.

- IT security methods and processes that protect internal and external Judiciary systems, services, and data against unauthorized use, disclosure, modification, damage, inaccessibility, and loss.

Strategic Priorities

The *Strategic Plan for the Federal Judiciary* includes the strategy, "Harness the potential of technology to identify and meet the needs of court users and the public for information service, and access to the courts," as well as four associated goals which form the basis of 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 a majority of its IT resources to sustaining legacy (sometimes outdated) technologies but, in order 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.

From January through June of 2022, more than 40 stakeholders from across the Administrative Office and the judiciary embarked on an effort to collaboratively create a modernization strategy which would serve as the roadmap for how the judiciary would invest resources to modernize its infrastructure, business applications, and workforce. The development of the modernization strategy was requested by the chair of the IT Committee, and several members of the Committee participated in the development, review, and approval of the modernization strategy. Once the modernization strategy was approved and published, several foundational modernization initiatives began, 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 formalize the development, approval, and implementation of 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 4.2 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. Future improvements to electronic public access to court records are discussed below and will be directly tied to the Case Management Modernization effort described on pages 3-5. The Case Management Modernization 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, 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 will play a role in the Judiciary's effort, now underway, to modernize CM/ECF and PACER. The Group will be actively engaged in the development process of the new PACER system. They will be invited to participate in regular user research sessions that will focus on requirements for various features of the new system as the project moves through the development lifecycle.

Case Filing/Case Management

Case Management/Electronic Case Files (CM/ECF): The federal courts' case filing processes are managed by 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 system as a result of the CM/ECF filing process.

The implementation of Next Generation (NextGen) CM/ECF modernizes the business processes used by the courts and judges' chambers. NextGen CM/ECF enhances the way judges manage cases by streamlining their processes and the ways they view information in the application. NextGen CM/ECF also enables 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.

All courts are now live on NextGen CM/ECF. Courts continue to upgrade to the latest two supported versions of NextGen CM/ECF at a fast pace. These upgrades improve the Judiciary's CM/ECF security posture. The NextGen releases 1.7.2 and greater will include the resolution of security

vulnerabilities and bug fixes based on priorities established by court expert panels. Finally, enhancements and new functionality have been added when required by new laws or direction from the Judicial Conference or other AO-sponsored advisory groups.

In 2019, the AO entered into an interagency agreement with 18F, a component of the General Services Agency that works with government entities on efficient and cutting-edge IT development, to conduct an independent assessment of NextGen. 18F conducted a full evaluation of the system, including a technical assessment and interviews with user groups. It determined that, for multiple reasons, the Judiciary's best path forward is to start fresh with an entirely new case management system and recommended that the Judiciary involve actual users in the development of the new system. Other key suggestions provided by 18F included: moving to the cloud; simplifying AO and court operations; adopting a DevSecOps culture, which would treat development, security, and operations as interrelated and mutually reinforcing practices; implementing data standards; and setting up an empowered cross departmental and cross functional team to develop the new modern CM/ECF product. The AO concurred with the recommendations made by 18F and put many of these recommendations into action in the Case Management Modernization initiative which focuses on the digital transformation of CM/ECF to build the Judiciary's next modern case management system. This digital transformation effort will be the main focus for the next few years.

As the focus is shifting to the Case Management Modernization effort, the judiciary is preparing for the eventual transition from NextGen to the new system. This strategic reallocation eventually will result in a "lights on" mode for NextGen where resources will be available to continue its secure operation, but changes or improvements will be 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.

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 IT applications maintained by the AO in support of the probation and pretrial services system have had significant problems with reliability and performance. To resolve these issues, the AO proposed a two-step plan to ensure the reliability and performance of PACTS and the related applications. The first step was to stabilize PACTS and existing applications while a replacement system is developed and deployed. The second step was to develop a replacement system for PACTS, using Software as a Service (SaaS) with a highly configurable platform solution. 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. Solicitation activities occurred in FY 2019 and a vendor was selected in April 2020. The PACTS replacement system (PACTS 360) development is currently underway and is scheduled to pilot and rollout the full operating capabilities the second quarter of FY 2024. Additional blanket purchase agreement (BPA) call orders will continue to be issued in 2023 and 2024. Operations and maintenance, including cybersecurity of the application, will begin with the initial rollout in FY 2024 and incrementally grow in the number of licenses required through FY 2025 and FY 2026. The program office is planning to issue additional call orders, if funding is available, in 2026 for the development of program management and advanced data

analytics capabilities to support the mission of the probation and pretrial services offices.

Jury Management

Jurors perform a vital role in the U.S. judicial system. Jury service is an important civic function that supports the right of trial by jury. The Constitution provides that the "trial of all crimes, except in cases of impeachment, shall be by jury." U.S. Const. art. III, § 2, cl. 3. 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 Windows-based jury management system for over 20 years, and it will soon become obsolete and will need to be replaced. It will be replaced with a web-based solution that is expected to be more cost efficient and easier to support. The web-based solution will be centrally managed to allow for better security. It also will contain better methods to respond to security vulnerabilities and will incorporate more periodic functional enhancements. Business requirements have been documented and the next step will be to procure software that can be designed, developed, and deployed through a partnership between Judiciary experts and a vendor who meets the Judiciary's 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).

Administrative Support

Several national administrative systems supporting finance, human resources, and facilities management are in the midst of modernization. The goal of these efforts is to deliver high-quality and secure solutions aimed at reducing costs, enhancing the user experience, and strengthening internal controls.

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' aging technical architecture poses significant IT risks and could potentially impact the availability of the application, compromise JIFMS' data integrity, and jeopardize the Judiciary's ability to address new financial management requirements.

The modernization of JIFMS is a priority for the Judiciary and efforts to upgrade JIFMS to the current version of the commercial off the shelf (COTS) solution is an ongoing, multi-year

initiative. This upgrade will provide enhanced functionality, improved system security, support for the latest infrastructure, and position the AO to deploy several government-wide solutions such as the Invoice Processing Platform (IPP)[2] and G-Invoicing[3] in the future. It will also resolve several known software defects. Once the upgrade is complete, a routine and predictable upgrade cycle can be established, allowing the Judiciary to take advantage of an up-to-date and supportable financial management solution into the future.

The Judiciary is pursuing a "back to baseline" strategy that involves minimizing Judiciary-specific customization of the underlying COTS solution. Minimizing customization should result in streamlined operations and maintenance activities and reduced complexity of future upgrades. It will also help achieve the goal of establishing a routine and predictable upgrade cycle.

Automated Collections Register (ACR): Deployment efforts are well underway for the ACR system to replace the various cash register systems used by district, bankruptcy, appellate and national jurisdiction courts. The deployment of ACR is another step towards the Judiciary moving to an enterprise platform that utilizes modern software and infrastructure. The solution is designed to integrate with the Judiciary's financial and case management systems. With the court community leveraging a single system, the Judiciary is well positioned to meet future legislative, business, and technological requirements. Full implementation of ACR is targeted for completion at the end of calendar year 2023.

---

[2] IPP is a web-based system that provides one integrated, secure system to simplify the management of vendor invoices.

[3] G-Invoicing is the long-term solutions for Federal Program Agencies to manage their intragovernmental Buy/Sell transactions; https://www.fiscal.treasury.gov/g-invoice/

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 their 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 begin after the completion of the JIFMS upgrade. Once the processes are documented, development and implementation activities will begin. The court community will participate throughout the initiative.

The JIFMS, ACR, and debt management efforts are designed to align with and complement 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 (GAAP). 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 uses HRMIS to process human resources (HR) transactions, including leave accruals, employee performance, benefits administration, and payroll processing. The Judiciary is focused on making system improvements to address regulatory and statutory requirements driven by the executive and legislative branches.

The AO is working closely with the court HR community to identify system enhancements that improve the efficiency and accuracy of their business processes. The AO is developing plans to increase court use of the optional employee performance management module. This effort includes developing communities of practice and focus groups to share information and gather feedback related to these products and to identify enhancements to make HRMIS an attractive alternative to local performance management solutions.

The AO is also using new technologies to deliver more valuable solutions to the Judiciary. This includes providing court units real-time access to leave data and the ability to leverage this data in local applications that support various business needs. The AO is also evaluating new solutions to create interactive dashboards utilizing HR data.

Now that a routine upgrade cycle for HRMIS is in place, the focus has shifted to taking advantage of the latest technologies available while minimizing the impact to the user community, optimizing new features, and maintaining an up-to-date, supportable human resources management solution into the future.

Fingerprint Transmission System: In a continued effort to improve and standardize the background check and investigations process, the AO procured a new fingerprint solution that will standardize how all court units and federal public defender organizations (FPDOs) enter and transmit biometric information for civil processes. The new solution will replace the current methods used to submit fingerprints for background checks (inked fingerprint cards and LiveScan fingerprints), increase data security, and improve the efficiency of the overall process. This new centrally maintained, web-based application does not store data locally. All data is securely transmitted to a central repository, providing better protection of personally

identifiable information. The new application began rollout in late FY 2022 and will continue through FY 2023.

Financial disclosure reporting: The Ethics in Government Act of 1978 requires all judicial officers and certain Judiciary employees to file financial disclosure reports. A new modernized, end-to-end financial disclosure system, the Judiciary Electronic Filing System (JEFS), is in development to meet the needs of Judiciary filers and those administering the program. JEFS will streamline the process of filing and amending reports and includes correspondence automation and tracking, redaction, and compliance within a single application. Additionally, a public site was developed and released on November 7th, 2022, that allows for the online request and release of financial disclosure reports to meet the Courthouse Ethics and Transparency Act.

Real estate and facilities management (Integrated Workplace Management System - JSPACE): The AO completed implementation of the real estate and facilities management system, JSPACE, in September 2022. JSPACE provides comprehensive data and analytics for the Judiciary to manage more than 40 million usable square feet of space in 800 locations with an annual rental cost of more than $1 billion. Furthermore, it supports the Judiciary's long-range facilities planning efforts and overall rent and space management function as well as the Capital Security Program,[4] Service Validation

Initiative,[5] and No Net New Policy.[6] The base space and lease functionality of the system has been deployed to all circuits. Additional capabilities including asset management, parking management, and strategic planning will be included in the enterprise solution.

Judiciary Vulnerability Management Information Services: The AO is committed to improving the ability of the Judiciary to assess and mitigate security and emergency management related risks to staff and facilities. This initiative was previously called the Judiciary Disaster and Recovery Tool (JDART). It began in FY 2020, providing the Judiciary a capability to visualize and analyze information regarding natural hazards impacting operations. As more risk-based needs were identified, additional information concerning public health, transportation, power, and threats to the Judiciary have been added. Additional data capture, analytical, and visualization services are being designed to improve local and national Judiciary situational awareness. As an example, these services were used extensively to provide data and insight into the impact of the COVID-19 pandemic.

Most recently, with the passage of the Daniel Anderl Judicial Security and Privacy Act, these services are being used to design and implement additional forms, analytical services, and visualizations to support monitoring the internet for covered information[7], removal of covered information,

---

[4] Endorsed by the Judicial Conference of the United States in September 2015, the Capital Security Program is designed to ameliorate security deficiencies in existing courthouses where physical renovations are viable, and the construction of a new courthouse is not needed or expected within the next 15 years.

[5] The Service Validation Initiative is a collaborative partnership between the Judiciary and the General Services Administration to improve all aspects of developing, designing, constructing, managing, and maintaining facilities.

[6] No Net New Policy—Any increase in square footage within a circuit needs to be offset by an equivalent reduction in square footage identified within the same fiscal year, subject to the following exclusions: new courthouse construction, renovation, or alterations projects approved by Congress.

[7] "Covered information" is a term used in the Daniel Anderl Judicial Security and Privacy Act of 2021 to refer to personally identifiable information and other data elements that can put judges and their families at risk.

coordination of threat management activities with relevant agencies, and reporting of judicial threats to the U.S. Marshals Service (USMS). The AO will also continue to explore additional solutions to strengthen analysis of security and emergency management issues, communications, and situational awareness during emergency situations.

Automation and Artificial Intelligence: The AO is in the process of adopting a standard set of development and integration platforms for administrative support systems. The platforms include low-code, robotic process automation (RPA) with artificial intelligence, application programming interface-centric integration, business intelligence, and workflow solutions. The goal is to leverage these tools to reduce the complexity of legacy custom solutions and replace them with standards-based platforms. These standards enhance security, improve quality, provide consumer-friendly user experiences, and reduce the time to market for administrative support products and services. The AO will incorporate the services and capabilities of these platforms into the service delivery model as the tools are adopted.

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. It covers caseload, defender, finance and 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 Categorization: To strengthen the IT security posture of the Judiciary and secure its data assets, a Data Security Categorization Workbook was developed for court units, federal public defender organizations, and national program offices. The AO led an initiative to identify, inventory, and categorize information types that are in common use across Judiciary systems. The resulting workbook sets minimum recommended categorization levels for Judiciary data, which can also be leveraged as part of zero-trust architecture. To help ensure that data is categorized consistently across the Judiciary's many systems, an update to the *Guide to Judiciary Policy* was approved by the IT Committee with a new requirement for court units and AO system owner offices to complete the workbook annually and submit it to the Judiciary Data and Analysis Office (JDAO).

Court Unit Dashboard: The dashboard is an interactive, easy to use, graphic display of court unit data that combines multiple sources of data (including caseload, staffing, IT deployments, and other relevant information) into a single interface, enabling powerful insights and enhanced analysis and reporting. In addition to the Court Unit Dashboard and caseload-specific dashboards available on JNet, there are two publicly available dashboards with bankruptcy caseload data and Bankruptcy Abuse Prevention and Consumer Protection Act report data that provide the public greater accessibility and visibility to bankruptcy data.

Data Literacy: This is defined by Gartner[8] 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. With an initial focus on the analytic tools available from the AO, 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: To continue its evolution towards self-service analytics and better governed data, the AO has procured and begun implementation of a new data management tool. This tool will support 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. In order to fully implement the tool, development is underway of custom integrations that are needed for the tool to interact with enterprise reporting and transformation tools.

Judiciary Data Working Group: The group was re-chartered in 2022 as a permanent subject matter working group and continues to include liaisons from three Judicial Conference committees that are significant stakeholders of data: the Committees on Information Technology, Court Administration and Case Management, and Judicial Resources.

---

[8] 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 details of how they carry out those processes can vary widely. Many of these variations reflect 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 allow 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[9] 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 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.

Efforts to leverage the national systems infrastructure that support locally developed administrative applications continue. These efforts present the opportunity for the Judiciary to leverage local court expertise and innovation to complement the national solutions and services delivered by the AO. Two examples are the Judiciary Inventory Control System (JICS), developed by the Northern District of New York district court, and JFinSys, a financial application developed by the Eastern District of Virginia bankruptcy court.

To promote Judiciary-wide technical and operational standards and enhance interoperability, a new lifecycle management process is being 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 has been developed and will be extended to include locally developed applications to avoid duplication of efforts, encourage

---

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

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 efficiently graduate software from the local to the national level and eventually to commercial cloud environments.

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

Increased demand on the Judiciary's communications networks both to support internal systems and to enable more widespread use of its public-facing technologies requires 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. Upgrading the data center core switching infrastructure has positioned the Judiciary for redundancy, failover capability, and stability over the next decade. The completion of the Wide Area Network (WAN) Diversity project increased the overall network availability and reliability through carrier diversity and redundant connections.

A new initiative on the horizon is Software-Defined Wide Area Network (SD-WAN), which will enable network administrators to match the behavior of the network environment to business priorities, routing traffic based on destination, application, and network status. With the advent of application centralization and data center consolidation as well as the move to commercial cloud providers, the WAN needs to become more dynamic and tuned for peak performance through maximizing the use of low-cost circuits for lower priority applications. The SD-WAN will provide the Judiciary the ability to dynamically and securely route, monitor, and measure real-time traffic to optimize performance. A plan is being developed to upgrade the data communications network (DCN) WAN router infrastructure to support this capability, including evaluation of the data center network infrastructure and development of architectural requirements needed to improve performance of the Judiciary's enterprise infrastructure.

Enterprise Operations Center

The Judiciary established the Enterprise Operations Center (EOC) in 2018 to provide 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

The network also provides a foundation for enhancing centralized hosting services. 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 provide 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 cloud will integrate the current on-premises Judiciary private cloud with readily available modern and secure commercial cloud offerings. The acquisition of commercial cloud services will allow the Judiciary to provision

modern cloud services to quickly meet individual business needs using a 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.

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. These technologies include evidence presentation, videoconferencing, assisted listening systems, and language interpretation systems.

Evidence presentation technology supplied by the court helps to level the playing field in the courtroom, preventing a mismatch of resources in which one litigant has the resources to make technologically advanced presentations and the other does not; such a mismatch could unfairly influence jurors' perceptions and the outcome of a trial.

Supplemental systems such as videoconferencing, assisted-listening sub-systems, and language interpretation sub-systems provide additional functionality to a courtroom audiovisual (AV) system that offers improved access to the justice system and has become a necessity to the dispensing of justice.

Judiciary-wide standards for courtroom technologies serve as a baseline for the introduction of current and next-generation tools and capabilities. Development of audiovisual over internet protocol (AVoIP) courtroom AV designs, along with proof-of-concept projects on technologies that will facilitate the efficiency of trials and hearings, are ongoing and include the following:

- AVoIP AV design standards. The AO is finalizing a statement of work for a new contract to develop the AV designs and standards. Within this project future networking capacity and impact issues will also be addressed.

- Speech-to-Text related solutions

  - Real-Time Translation (RTT) for digitally recorded proceedings

  - Automated cloud-based Artificial Intelligence (AI) solutions

  - Digital recording to transcript solution utilizing AI and cloud-based applications for Civil Proceedings

- Remote Court Reporter solutions, for which a court reporting shared services program framework is being established

- Secure and FedRAMP compliant remote RTT solutions

- Automated audio storage of court proceedings cloud-based, configured control systems (potentially replacing programmed control systems)

- Cost reduction solutions

- Training solutions, including a Courtroom Technology Training SharePoint site

- Virtual Courtrooms based upon an Electronic Sound Recording (ESR) solution

In addition, the Telephone Interpreter Program (TIP) is being updated to reflect newer technologies being utilized by the courts and to ensure that a hardware/software manufacturer solution is in place for the future.
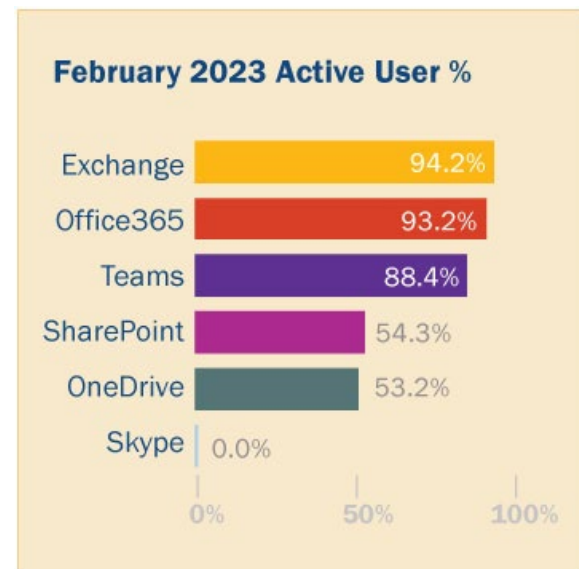
Improvements and efficiencies are being realized from digital video as well as the centralization of audio, video evidence presentation, and videoconferencing systems.

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. Current supply chain issues are also impacting maintenance and new courtroom technology installations.
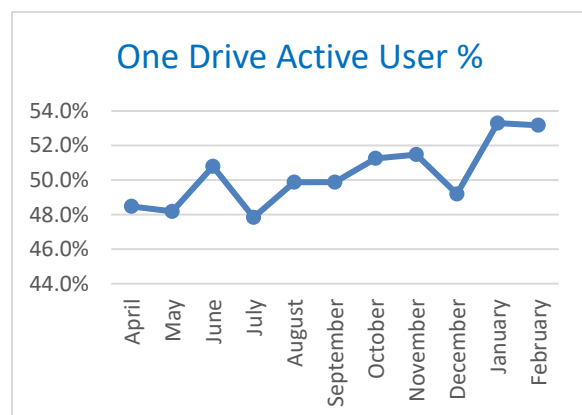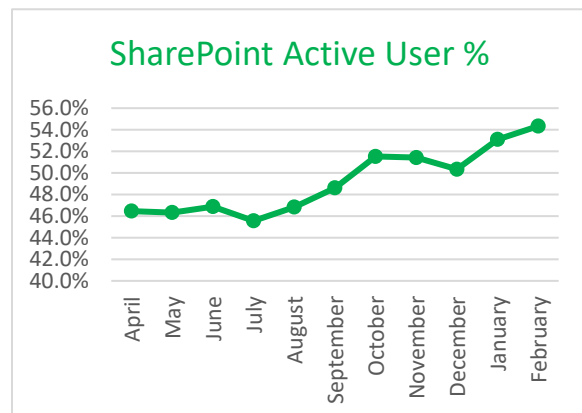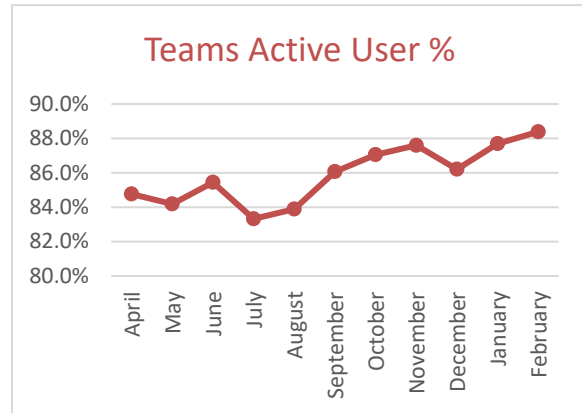
Communications

The adoption of the Microsoft Office 365 communication and collaboration platform deployed in 2019/2020 continues to grow across the Judiciary. Microsoft Office 365 provides Judiciary users the ability to access email, collaborate on documents, and communicate with co-workers from desktop computers, laptop computers, tablets, and mobile devices. Windows and iOS devices are primarily used to connect to the Office 365 environment; however a small percentage of users access the environment using Mac or Android based devices.

The active user percentage for Exchange (also known as Outlook) remains steady, and there has been an increase in the active user percentages for Microsoft Teams, SharePoint Online, and One Drive over the past year.

February 2023 Active User %

Exchange	94.2%
Office365	93.2%
Teams	88.4%
SharePoint	54.3%
OneDrive	53.2%
Skype	0.0%

As the adoption of Microsoft Office 365 continues to grow, the several legacy communication and collaboration tools have been successfully sunset, including AT&T WebEx, Quickr, Connections, Skype for Business, NVTCS, Documentum, and SharePoint on-prem. The AO will continue to make Cisco WebEx and AT&T Audio conferencing available to the courts through late 2023 or early 2024.

Teams Active User %

SharePoint Active User %

One Drive Active User %

As Microsoft continues to add additional features to the Office 365 platform, the AO will continue to evaluate how to leverage those capabilities throughout the Judiciary. The focus will be on user adoption of Office 365, Microsoft Outlook, and OneDrive, while new tools such as Microsoft Teams, PowerAutomate, PowerApps, Stream, and Delve are introduced.

SharePoint Online (SPO) is the main collaboration and document management tool within Microsoft's Office 365 platform. SPO supports 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 implementation which was scheduled to be completed in July 2021, but as of April 2023, there remain approximately 65 courts that are in progress to complete SPO onboarding. The focus in 2023 is to complete the implementation of SPO across the Judiciary and increase adoption of the Office 365 functionality by leveraging Teams as well as SPO to improve communication and collaboration. The SPO Center of Excellence (SPOCOE) will continue to provide assistance across the Judiciary by featuring information such as the Office Hours series of weekly presentations/webinars, SharePoint Sherpa Services, Judiciary/court-unit specific use cases, SPO governance/ guidance, and best practices. The team will continue to present, as requested, at Judiciary conferences to promote SharePoint education and functionality. One activity being explored is a biennial SharePoint conference where Judiciary users share best practices with one another, including solutions, applications and workflows developed using SPO that may be applicable to many other court units.

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 DCN, 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 simply to cause embarrassment, 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 and information through preventative measures. Network- and host-based systems are employed to routinely inspect traffic 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 DCN as well as between the DCN and the internet—further prevent breaches (as do network access controls, endpoint protection systems, encryption solutions, and patch management solutions). 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: AO efforts to better understand and categorize the various data and systems at court units and AO national program offices based on their security sensitivity revealed a need to accelerate periodic assessments of local IT security programs. Based on government and industry best practices for periodic independent assessments of high, moderate, and low impact systems, at the rate of every three, five, and seven years respectively, efforts are needed to accelerate mandatory court unit security assessments from a five-year cycle to a three-year cycle due to the validated categorization of high impact systems resident at all court units.

Secure coding practices in Judiciary applications: In 2022, 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) tool to track vulnerabilities, findings, plans of action and milestones and risk acceptance.

Blue Team service: In 2021, the AO started providing Blue Team services as an optional addition to AO Red Team services. 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: This centrally managed service enables courts and national program offices to collect, retain, search, alert, report, and analyze large volumes of computer-generated log messages in real-time to identify and troubleshoot both general and security-related IT incidents. This service is one of the primary tools being utilized by the EOC to respond proactively to identified issues before they impact the national infrastructure. National adoption of this service across all courts was mandatory in 2022.

Judiciary firewall service: The Judiciary has installed a dedicated security appliance (firewall) to the boundary between each court and the DCN, reducing the likelihood that a malicious event will spread laterally among courts. Its placement ensures a consistent configuration across locations and complements the security infrastructure at the Judiciary data centers. The Judiciary has implemented additional capabilities of 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: Network segmentation is a core principle of ZTA that will enhance the security of network resources by restricting access to specific network segments based on user access authorization and on the health and/or location of the device attempting to connect to them, only allowing access to the minimum network resources required to perform a given function or task. This initiative will be conducted in an incremental, phased approach with the initial focus being on segmentation of internet data center (IDC) resources. Results obtained during this initial phase will be used in formulating subsequent phases and culminate in segmentation of all DCN resources.

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 and a comprehensive plan for implementing MFA through a phased approach is under development.

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 virtual private network (VPN) service. Upon implementation, a 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, in order 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: In order 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 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, continues to evolve and 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. 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 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. Efforts are underway to gain access to classified data and systems to better coordinate with the Intelligence Community and 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 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 will 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" all 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 on the next page shows the Judiciary's anticipated IT resource requests for FYs 2024 through 2028, organized by category within the Judiciary Information Technology Fund (JITF).[10] Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

---

[10] 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

JITF Program Component	Current Estimate (Dollars in Millions)				
	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028
Administrative and Mgt Systems	74.9	84.5	107.5	138.8	141.6
Court Administration and Case Mgt	27.8	26.0	50.4	53.1	43.9
Court Allotments	126.8	125.8	131.0	133.0	134.5
Court Support	114.3	122.9	127.7	130.2	132.9
Cybersecurity & IT Modernization Plan	156.7	122.0	124.7	133.5	138.7
Infrastructure and Collaboration Tools	150.8	146.7	210.8	195.1	205.7
Judicial Statistics and Reporting	10.7	14.3	16.2	16.9	13.8
Telecommunications	108.7	128.6	133.5	115.7	120.6
Subtotal	770.8	770.8	901.8	916.3	931.7
Electronic Public Access Program	210.0	218.5	223.6	225.3	230.2
Total JITF Financial Requirements	*980.8*	*989.3*	*1,125.4*	*1,141.6*	*1,161.9*

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 and 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; 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.