# Fiscal Year 2023 Update

# Long Range Plan for Information Technology in the Federal Judiciary

Approved by the Judicial Conference of the United States

September 2022

# Long Range Plan for Information Technology in the Federal Judiciary: Fiscal Year 2023 Update

## Table of Contents

# Introduction

The Strategic Plan for the Federal Judiciary 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) 2023 through FY 2027. 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:

1. 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.
2. Internal Judiciary systems used by judges and chambers, court staff, probation and pretrial services officers, and AO personnel.
3. 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.
4. 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.

## 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 3.8 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, but longer term improvements to this program will be directly tied to the CM/ECF modernization effort described on pages 4-5.

*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. These recommendations have resulted in significant changes to EPA services, including:

- Implementing enhanced Case Title and Party Name fields in the PACER Case Locator, allowing the public to search using one character in combination with a wildcard character.
- Resolving issues with viewing PDFs on iPads (for District CM/ECF) in NextGen CM/ECF Release 1.7 in Fall 2021.
- Adding "coverage dates" available by court to the PACER Case Locator, providing the date range of cases that users can find when searching each court's CM/ECF database.
- Releasing a Pro Se User page on PACER.gov, making it easier for the public to understand how to access and use PACER.
- Encouraging increased court use of Really Simple Syndication (RSS) feeds in CM/ECF through outreach to help courts overcome obstacles with, and raise awareness of the public access benefits of, using RSS feeds more fully. These benefits include providing timely notifications about court filings to keep public subscribers apprised of case activity in various jurisdictions of interest.

*Redesigned PACER Website.* At the end of June 2020, a redesigned PACER website was released. Progress in updating the public-facing applications accessible from the PACER website continues to provide a more consistent and unified user experience in the areas of authentication, billing, and account management.

*PACER User Assessment.* In 2021, the AO conducted a PACER User Assessment to measure user satisfaction with PACER services and identify areas for improvement. The results of the 2021 assessment show that 84 percent of users are satisfied with the PACER services offered and the value of the services for the fees charged. The assessment's findings point to areas that could have a significant positive impact on user satisfaction, including improved search capabilities and greater awareness of available services. The AO will use the results of the survey to inform future improvements to public access services and has begun quarterly user assessments, which are more focused and targeted to specific areas for improvement.

*New PACER Case Locator and PACER Authentication Application Programming Interfaces (APIs).* In December 2020, the AO hosted a virtual town hall for public users to discuss the release of the PACER Case Locator API and asked for volunteers to assist with testing the API. The new API, which was released on September 19, 2021, makes it easier for those using automated scripts to consume data from the PACER Case Locator. During this time, the PACER Authentication API, which simplifies the use of automated scripts to access PACER, was also released.

## 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 appellate and bankruptcy courts are live on NextGen CM/ECF. As of April 15, 2022, there were 191 courts live on NextGen (13 appellate courts, 88 district courts, and 90 bankruptcy courts), and another four district courts have signed up for implementation by the end of June 2022.

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.

NextGen currently dedicates most of its IT resources to maintaining aging technology, but in order to take advantage of advances in technology and to protect the Judiciary from cyberattacks, the Judiciary must take meaningful steps to modernize its IT systems. In December 2020, the AO entered into an interagency agreement with 18F[1] to assess NextGen. The first phase of the assessment, the Path Analysis phase, was completed in March 2021. During this phase, 18F provided the AO with a roadmap for the future. 18F completed the second phase of the assessment, the Experiment & Iterate phase, and submitted a report including recommendations that the Judiciary needs to implement to achieve the digital transformation of CM/ECF. After completion of the second phase, the AO and 18F continued working together through early 2022, with 18F focusing on the development of concrete approaches to breaking down the AO's institutional siloes and assisting the AO in adopting a DevSecOps culture. A DevSecOps culture would treat development, security, and operations as interrelated and mutually reinforcing practices. 18F's engagement with the AO ended shortly after delivery of its final supplemental report, dated January 31, 2022,

1 *18F is a technology and design consultancy for the U.S. Government, inside the government. 18F partners with agencies to improve the user experience of government services by helping them build and buy technology.*

titled "How to get started building a new CM/ECF. Today."

In the final supplemental report, 18F made a total of 10 recommendations and the Judiciary concurs with all of them. The Judiciary is conducting market research to explore available options for accelerating the digital transformation of the CM/ECF system. The Judiciary is committed to building a new system with modern technology and architecture that: is cloud-based; incorporates simplified AO operations; includes court-level innovation; adopts application program interface (API) architecture with standards and common schemas; and adopts a DevSecOps culture (see page 22). The digital transformation of CM/ECF requires cross-functional and cross-departmental teams working with real users and domain experts to build the new system. All future contracts for the digital transformation must incorporate Quality Assurance Surveillance Plans (QASPs).[2]

*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 commercial off-the-shelf (COTS) products as well as 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 expected to be 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 last quarter of FY 2023. Additional blanket purchase agreement (BPA) call orders will continue to be issued in 2022, 2023, and 2024. Operations and maintenance, including cybersecurity of the application, will begin with the initial rollout in FY 2023 and incrementally grow in the number of licenses required through the first quarter of 2024. The program office is planning to issue additional call orders, if funding is available, in 2024 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. system of justice. 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 must update its 20-year-old, Windows-based jury management system because it will soon become obsolete. It will

[2] Quality Assurance Surveillance Plans are used by the federal government to assess contractor performance.

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 a quicker response to security findings 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 to meet 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 Systems

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 the Judiciary's single official accounting system of record, serving as a decision support management information system and supporting the Judiciary's core accounting, procurement, and debt management functions. JIFMS provides enhanced interfaces with external systems, improved data sharing capabilities, improved internal controls, and standardized business practices. 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 AO has completed the planning and analysis phases as part of the strategic direction for the modernization of the JIFMS product to a current version of a COTS solution. 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)[3] and G-Invoicing[4] 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 AO 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

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

4 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/.

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 underway for the ACR system to replace the various cash register systems used by district, bankruptcy, appellate and national jurisdiction courts. Currently, the cash register function is decentralized with a variety of solutions being used throughout the Judiciary. Many of these solutions are obsolete and are challenging to maintain due to aging technology.

The development of ACR is another step to unify the Judiciary on a single platform, utilizing modern software and infrastructure that can be supported nationwide. The solution is designed to integrate with the Judiciary's financial and case management systems. With the court community leveraging a single system, the AO can further meet future legislative, business, and technological requirements.

*Debt management:* The Judiciary is pursuing 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 this functionality 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 around financial case management. It will offer debt management functionality for the district and bankruptcy court community. Efforts are currently underway to identify and define key business processes. Once these processes are defined, requirements will be gathered, followed by development and implementation activities. The AO is actively engaging with the court community on this 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 imitative 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 AO 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 our HR business partners to identify system enhancements that will improve the efficiency and accuracy of their business processes, including the goal of increasing the adoption rate of the national leave system, HRMIS Leave Tracking, to 100 percent. It is estimated that by the end of FY 2023, the Judiciary will be at 91 percent of this goal and the AO, working with the HR business partners, will assist with encouraging the remaining courts to adopt this consolidated national leave system. The AO is also 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 evaluating new technologies to deliver more valuable solutions to the Judiciary. This includes providing court units real-time access to their leave data and the ability to leverage the data in local applications that support various business needs. Another example is evaluating new solutions to create interactive dashboards of HR data.

Now that the AO has established a routine upgrade cycle for HRMIS, the focus has shifted to defining a modernization roadmap to ensure that the Judiciary is 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 continuing effort to improve and standardize the background check and investigations process outlined in the *Guide to Judiciary Policy,* Volume 12 (Human Resources), Chapter 5 (Employment), § 570 Background Checks and Investigations, the AO has procured a new fingerprint solution that will standardize how all court units and Federal Public Defender Organizations (FPDOs) enter and transmit biometric information. 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 and all data is securely transmitted to a central repository, providing better protection of personally identifiable information. The new application will begin rollout in late FY 2022 and continue through FY 2024.

*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 new public site will be integrated with JEFS to allow for the online request and release of financial disclosure reports.

*Real estate and facilities management (Integrated Workplace Management System - JSPACE):* Efforts are underway to implement a COTS real estate and facilities management system to replace disparate systems and tools used today. The new system, called 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 $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,[5] Service Validation Initiative,[6] and No Net New Policy.[7] Space and

[5] 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 (JCUS-SEP 2015, p. 32; JCUS-SEP 2020, p. 37).

[6] 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.

[7] 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 (JCUS-SEP 2013, p. 32; JCUS-SEP 2014, p. 29).

lease functionality deployment to all circuits is anticipated by the end of FY 2022. Additional capabilities will be deployed between FY 2023 – FY 2026.

*Judiciary All-Hazards Risk & Vulnerability Analysis Service (JARVAS):* The AO is committed to improving the ability of the Judiciary to prepare for and respond to threats to staff and facilities. The JARVAS initiative, formerly known as the Judiciary Disaster and Recovery Tool (JDART), began in FY 2020 to provide the Judiciary with the capability to monitor threats and hazards, vulnerabilities, and other information impacting operations. JARVAS also provides reporting of specific incidents through data visualization tools designed to improve local and national Judiciary situational awareness. Information for assessing and monitoring a wide range of threats including potential natural, technological, biological, radiological, public health, and human-initiated hazards is captured and analyzed using JARVAS. Based on current geographic information system technology, the new tools will provide a single operational view of developing emergency situations, such as natural or human-made disasters. The new tools will help Judiciary decision-makers and emergency personnel quickly and effectively assess and respond to evolving situations. JARVAS has been used extensively to provide data and insight into the impact of the COVID-19 pandemic. The AO will also explore additional solutions to strengthen communications and situational awareness during emergency situations.

*Automation and Artificial Intelligence:* The AO is 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, service bus[8]for 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 standard-based platforms that 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 ser-vices; 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

[8] A service bus is a software platform used to distribute work among connected components of an application.

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, data security categorization workbooks were developed for court units and national program offices. Workbooks are currently under development for federal public defender organizations. The AO led an initiative to identify, inventory, and categorize information types that are in common use across Judiciary systems. The resulting workbooks help ensure that data is categorized consistently across the Judiciary's many systems by setting minimum recommended categorization levels for Judiciary data, which can also be leveraged as part of zero-trust architecture.

*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, new dashboards with publicly available bankruptcy caseload data and Bankruptcy Abuse Prevention and Consumer Protection Act report data provide the public greater accessibility and visibility to bankruptcy data.

*Data literacy*: This is defined by Gartner[9] 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

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

better governed data, the AO has procured and begun implementation of a new data governance 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, procurement 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.

## 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.

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[10] 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

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

by the Eastern District of Virginia bankruptcy court.

To promote Judiciary-wide technical and operational standards and enhance interoperability, a new technical standards management process is being developed for all Judiciary IT systems. Furthermore, a catalog of national applications has been developed and will be extended to include locally developed applications to avoid duplication of efforts, encourage collaboration, highlight gaps in the functionality of national applications, and promote communities of practice and technology knowledge-sharing. Finally, technology solutions are being developed to efficiently deploy 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 self-provision computing resources to quickly meet individual business needs on a pay-as-you-go basis. 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
- 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
- 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
- Virtual Courtrooms based upon an Electronic Sound Recording (ESR) solution

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 Judiciary successfully deployed Microsoft Office 365 in late-2018 and completed all email migrations from Lotus Notes to Outlook by January 2020. Judiciary users were just starting to get comfortable with the enhanced collaboration tools provided with the Office 365 suite (Outlook, OneDrive, and Skype for Business) when the pandemic hit, forcing mandatory telework situations for most users. The AO responded quickly to roll out Microsoft Teams, converting in-person training sessions to virtual training, developing new training courses for Teams, and offering refresher courses for the National Video Teleconferencing Service (NVTCS) and WebEx. The adoption rate for Microsoft Teams grew quickly, and Skype for Business was sunset in July 2020.

While Microsoft Teams is being used extensively for internal collaboration, it initially did not have all of the functionality needed to conduct virtual court operations. The AO conducted an extensive requirements-gathering initiative to evaluate the various communication and collaboration tools that were being used across the Judiciary. The primary objective of this evaluation was to determine if the Judiciary was funding multiple tools that provided the same capabilities. As a result of this evaluation the following communication and collaboration tools have been shut down – AT&T WebEx, Quickr, Connections, and Skype for Business. The legacy NVTCS functionality was first moved to Cisco CMS, and then NVTCS was sunset in December 2021.

Since the rollout of Microsoft Teams in 2020, Microsoft has added more than 200 new features to the product including Breakout Rooms and Co-Organizer Capabilities. The AO deployed a tool called “Pexip” in January 2022 that provides the capability for non-Microsoft

video endpoints to join Teams meetings. Courts are still utilizing other video conferencing services to provide toll-free call-in options and to enable simultaneous interpretation.

The AO will continue to make Cisco WebEx and AT&T Audio conferencing available to the courts thru late 2023 or early 2024.

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 2022, there remain approximately 100 courts that are in progress to complete SPO onboarding. The focus in 2022 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 Office Hours series of presentations/webinars, Sherpa Services, Judiciary/court-unit specific use cases, SPO governance/guidance, and best practices. The team will be presenting at various conferences [e.g., Automation Training Community of Practice (ATCoP)] to promote education and functionality of SPO. One activity being explored is to hold an SPO conference where Judiciary users can share best practices with one another, including 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 interrupt, destroy, or threaten the delivery of essential services. Addressing these threats requires the use of multiple measures in the

following areas: 1) preventing malicious activity; 2) detecting, analyzing, and mitigating 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 improvement to adapt to the ever-changing threat environment and helps ensure that resources are focused where they provide the most benefit. The resulting data are 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 segmentation techniques, security policies, privilege management, 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:

*Annual IT security self-assessments*: Each Judiciary unit (court unit and FPDO) assesses the effectiveness and maturity of its local IT security program using a common rubric. Results are submitted locally, at the circuit level, and to the national program for analysis and potential identification of areas for improvement in both the local and national security program. The areas assessed by this program evolve over time to incrementally improve the security baseline and to address emerging threats. The fifth annual Judiciary unit self-assessment period concluded in December 2021. Based on an analysis of data collected to date, including validations performed of 2020 results during the mandatory independent court unit IT security assessments, the AO has made minor refinements for the upcoming self-assessment period. Additionally, each national program office assesses the effectiveness and maturity of security programs supporting national systems, such as case management (CM/ECF and PACTS), JIFMS, and identity management.

*Mandatory independent court unit IT security assessments*: This program launched in 2018. Due to budget constraints in 2020, the assessment cycle for courts was temporarily extended from at least once every five years to once every seven years. Full funding expected for FY 2023 will allow assessment cycles to return to once every five years. Each court unit

receives a comprehensive independent assessment of its management, technical, and operational safeguards to understand its strengths and weaknesses. Court units also receive feedback on the efficacy of the self-assessment program within their court unit. Assessed court units document the actions they plan to take in response to identified risks and share their action plans with the assessment team.

*Secure coding practices in Judiciary applications*: In 2018, the AO focused more closely on integrating secure coding practices into Judiciary software development, expanding the program with additional personnel and a more comprehensive objective. New static code analysis tools and open-source library vulnerability scanning software have allowed the AO to better prevent and detect coding vulnerabilities in judicial applications. Dedicated AO personnel regularly engage with court and national program software development teams to educate, assist in the integration of these tools in software builds, and to emphasize the importance of secure software development throughout the full lifecycle of applications. In 2020, the AO included secure coding metrics in the National System IT Security Scorecard, reinforcing the importance of this program and acquired security tooling to allow developers to make risk-based decisions on what open source software to integrate into their solutions.

*Increasing the use of the web application firewalls (WAF):* In 2022, to better protect internet-facing Judiciary web applications from malicious activity, the AO mandated the utilization of a WAF for all CM/ECF and PACER systems. WAFs provide a finer granularity of protection for web-based applications and can also be used to temporarily address some web vulnerabilities until they can be corrected in the application itself. Courts utilizing WAFs are better protected from malicious web traffic and external screen-scraping software that detrimentally affects the performance of court websites.

*Judiciary Vulnerability Management:* Starting in 2021, the AO developed a coordinated vulnerability management program leveraging DHS CISA 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.

*Enhanced network traffic analysis*: Upgrades to network monitoring devices and security appliances conducted in 2022 enabled the capture and filtering of network traffic to detect and contain potentially malicious activity across the Judiciary's CM/ECF and PACER environments. Additional upgrades across the DCN are planned as funding becomes available.

*Blue Team service:* In 2021, the AO started providing Blue Team services as an optional addition to AO Red Team services (described below). 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.

*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 main tools being utilized by the EOC to move toward proactively acting on identified issues before they impact the national infrastructure. National adoption of this service across all courts is mandated by 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, tailoring security policies will be vital in maximizing the utilization of the service.
*Zero-trust architecture (ZTA):* The Judiciary is moving toward a zero-trust architecture, an information security model that 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) and 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 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.

*Data management*: The Judiciary continues to seek ways to more effectively collect data, analyze it, and translate it into actionable information. For example, within the national IT security program, the AO applies data visualization and risk management tools to the annual court unit IT security self-assessment data and national system security self-assessment data to understand the impact of national IT security investments on enterprise security. These methods also help the AO to identify areas in which the self-assessment process supporting documentation needs improvement.

*Enhanced Endpoint Security:* Introduction of Endpoint Detection and Response capabilities to augment digital forensics 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.

*Forensics*: Digital forensic analysis is pivotal in determining the timeline and root causes of critical security incidents. Investments since FY 2020 have significantly improved the ability of security analysts to triage potential intrusions in order to prioritize investigations and identify the vulnerabilities exploited by hackers that require immediate remediation.

*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:

*Vulnerability Prioritization:* The AO plans to improve the Judiciary's ability to identify and prioritize remediating the vulnerabilities that pose the highest risk to Judiciary systems and networks. This process involves correlating vulnerability threat information with data from existent scanning tools, alerting courts and national programs about the increased risk of these particular vulnerabilities, and, when necessary, initiating additional out-of-cycle remediation processes.

*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.

*Standardized security tools*: Data from the Judiciary's cybersecurity efforts is continually analyzed to assess the need to modify or add tools to reduce risk. The underlying toolset comprising the Insight Program—the AO's approach that establishes a single pane of operational control (dashboard)—will be normalized and optimized to improve effectiveness in supporting Judiciary cybersecurity requirements. Rollout of these toolsets is complete. Courts were required to adopt the following nationally offered IT security services no later than March 31, 2022: Vulnerability Scanning, Patch and Asset Management, National Logging, Web-Based Threat Protection, Endpoint Protection, and Mobile Device Management.

*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.

*Development, Security, and Operations (DevSecOps):* In order to standardize and better secure IT systems which are custom developed for the Judiciary, the AO is undertaking an effort to adopt a DevSecOps application development methodology. DevSecOps is a commonly used methodology in commercial and government organizations and is beneficial by incorporating IT security practices throughout all aspects of the application development process so that security is "baked in" as opposed to being treated after-the-fact. Currently, AO program offices are in various stages of adopting Agile as a development methodology, and none have fully transitioned to the DevOps methodology. Transitioning to DevSecOps will be a major cultural shift for the organization, regardless of how necessary it may be.

# 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 below shows the Judiciary's anticipated IT resource requests for FYs 2023 through 2027, organized by category within the Judiciary Information Technology Fund

## Resource Requirements

| | Current Estimate (Dollars in Millions) | | | | |
|---|---|---|---|---|---|
| JITF Program Component | FY 2023 | FY 2024 | FY 2025 | FY 2026 | FY 2027 |
| Administrative and Mgt Systems | 82.3 | 99.4 | 116.0 | 118.6 | 115.4 |
| Court Administration and Case Mgt | 62.1 | 60.2 | 56.6 | 45.5 | 44.1 |
| Court Allotments | 112.7 | 121.4 | 123.2 | 125.1 | 122.0 |
| Court Support | 91.3 | 96.8 | 120.4 | 122.8 | 125.2 |
| Infrastructure and Collaboration Tools | 161.6 | 195.2 | 229.5 | 229.9 | 228.2 |
| Judicial Statistics and Reporting | 12.9 | 14.3 | 16.0 | 12.3 | 12.6 |
| Telecommunications | 137.3 | 155.7 | 162.4 | 140.4 | 129.8 |
| **Subtotal** | 660.2 | 743.0 | 660.2 | 743.0 | 660.2 |
| Electronic Public Access Program | 182.2 | 175.6 | 209.7 | 200.0 | 182.0 |
| **Total JITF Financial Requirements** | 842.4 | 918.6 | 1,033.8 | 994.6 | 959.3 |

(JITF).[11] Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

## 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; tools 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, LAN 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.

### 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.

[11] 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.

**Administrative Office of the U.S. Courts**

One Columbus Circle, N.E.
Washington, D.C. 20544

**www.uscourts.gov**