Fiscal Year 2021 Update

Long Range Plan for Information Technology in the Federal Judiciary

Approved by the Judicial Conference of the United States

September 2020

Contents

Introduction

2021

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 by which they do their jobs. As business processes and technology solutions have become interwoven, the Judiciary recognizes that IT presents opportunities not simply to replicate old paper processes in digital form but to reengineer many aspects of those processes altogether.

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 the IT program over the next three to five years, and summarizes the Judiciary's anticipated IT resource requirements for fiscal years (FY) 2021 through 2025. The strategic priorities discussed in this document integrate the *Strategic Plan for the Federal Judiciary*, as updated in 2015, 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, policies, and programs that ensure the quality and reliability of the Judiciary's IT services.
- IT security methods and processes that protect internal and external Judiciary systems, services, and data against unauthorized use, disclosure, modification, damage, inaccessibility, and loss.

[1] *Strategic Plan for the Federal Judiciary*, approved by the Judicial Conference of the United States, September 2015.

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 and maintain 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 and more fully utilize local initiatives to improve services.
- Develop system-wide approaches to the utilization of technology to achieve enhanced performance and cost savings.
- Refine and update security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information.

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

Continue to build and maintain 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 performance 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 in order 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 replacement of systems.

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.

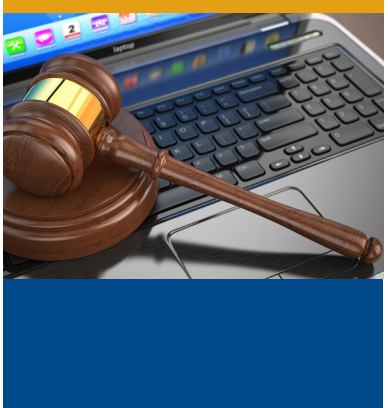
Electronic Public Access

The Judiciary provides electronic access to case information, including the documents in case files, through its Public Access to Court Electronic Records (PACER) System. 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 three 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 that restrict access to certain types of cases, information, and documents.

The Judiciary's Electronic Public Access (EPA) program established a Public User Group to provide advice and feedback on ways to improve PACER and other electronic public access services provided by the Judiciary. The EPA program is also redesigning the PACER.gov website. 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.

Case Filing/Case Management

The federal courts case filing process is managed by the Case Management/Electronic Case Files (CM/ECF) System, through which 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 file document availability through the PACER system as a result of the CM/ECF filing process.



The implementation of Next Generation CM/ECF (NextGen) modernizes the business processes used by the courts and judges' chambers. NextGen enhances the way judges manage case information, providing the information they need to work with minimal additional effort. NextGen 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 systems and between internal and external systems; supports a more consistent user experience for external users of the case management system; 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 courts are live on NextGen CM/ECF. Implementation waves for district and bankruptcy courts began in January 2018, and quarterly implementation waves, with 15 courts in each, began in July 2018. By 2021, the last wave of courts is anticipated to begin the implementation process to migrate to NextGen CM/ECF.

There will be at least one new NextGen and one Current Generation CM/ECF (CurrentGen) release per year for each court type. The CurrentGen releases will implement security updates and address any necessary required changes (due to new rules, for example). The NextGen releases will also include the resolution of security vulnerabilities and bug fixes based on priorities established by court expert panels. Finally, enhancements and new functionality may be delivered if required by new laws or direction from the Judicial Conference.

The Probation and Pretrial Case Tracking System, also known as 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 is to stabilize PACTS and existing applications while a replacement system is developed and deployed. The second step is 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, including a data migration strategy, occurred in FY 2019. A vendor was selected in April 2020.

Jury Management

Jurors perform a vital role in the U.S. system of justice. Jury service is an important civic function that supports one of the most fundamental rights of individuals—the right to have the interests of justice reviewed and determined by fellow citizens. 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 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 be replaced with a web-based solution, which will be less expensive and easier to maintain and operate. The web-based solution will be centrally managed to allow for a quicker response to security findings and more regular technical enhancements. Business requirements have been documented and the next step will be to procure software that can be customized 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 is introducing efficiencies to judges' chambers. New features have been developed, such as the Judge Review Packet which provides 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 actions. Judges and their staff will also have the advantage of utilizing a user interface called Workspace, which provides customizable screen content based on job function. Mobile Briefcase allows appellate judges and their staff to download and edit documents on a tablet computer. 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). An integrated calendar for district and bankruptcy judges began as a proof of concept in 2018. The Calendar module, one of the most complex components of the new system with over 2,000 requirements defined by judges and court staff, is currently being piloted by one district court (N.D. Fla.) and three bankruptcy courts (Bankr. D. Alaska, Bankr. D.N.J., and Bankr. D. Or.). Testing of the Calendar module has been moving slowly, however, with delays in preparing and developing the software to allow the pilot courts to go live on the module. Considering these issues and others, it is uncertain whether the Calendar module will be released broadly.

Administrative Support

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

Deployment of the Judiciary Integrated Financial Management System (JIFMS) has been completed, and it is now in use throughout the Judiciary supporting the core accounting and procurement functions. In May 2020, debt management functions in JIFMS will also be fully deployed nationwide. JIFMS provides enhanced interfaces with external systems, improved data sharing capabilities, improved internal controls, and standardized business practices.

The AO is now positioned to upgrade the JIFMS product to the latest version. This upgrade will provide enhanced functionality, 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 completed, a routine and predictable upgrade cycle will be established, allowing the Judiciary to take advantage of an up-to-date and supportable financial management solution into the future.

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

Development efforts are also underway for an Automated Collections Register (ACR) system to replace the various systems used by district, bankruptcy, and appellate courts. Currently, the cash register function is decentralized with a variety of different cash register solutions being used throughout the Judiciary. Many of the solutions being used today are obsolete and difficult to maintain due to aging technology. The development of the ACR system is another step to unify the Judiciary on a single platform, utilizing up-to-date software and infrastructure that can be supported nationwide. The solution is being 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.

Lastly, the AO is pursuing a unified debt management solution that will replace the Civil/Criminal Accounting Module, which is currently integrated into JIFMS and other debt management solutions used throughout the Judiciary. This solution 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 are defined, requirements will be gathered, followed by development and implementation activities. The AO is actively engaging with the court community and the Financial Managers Working Group on this initiative.

Each of the efforts is designed to align with, and complement, a five-year Judiciary strategic effort called the Judiciary Data Integrity, Reporting and Controls (JDIRC) program, to produce annual financial statements for the Judiciary that are audited, and consolidated in a standardized way throughout the Judiciary. The JDIRC program will transform financial reporting requirements across the Judiciary, improve the Judiciary's internal controls programs, and strengthen the integrity of Judiciary financial data.

The Human Resources Management Information System (HRMIS) manages human resources transactions, including leave tracking, employee performance, and payroll production for the Judiciary. The AO is focused on making system improvements to address regulatory and statutory requirements driven by the executive and legislative branches. In addition, efforts are underway to enhance the utilization of the non-mandatory modules of HRMIS, Leave Tracking and ePerformance. Plans call for establishing communities of practice and focus groups to share information and gather feedback related to these products and make them attractive alternatives to local development or procurement efforts. Additional goals include improving training and communications about HRMIS.

Recognizing the importance of "people" data supporting other solutions and capabilities, the AO continues to explore opportunities to provide such data so that it can be used appropriately by other systems in accordance with Judiciary data governance principles.

Similar to the financial systems, the AO is focused on establishing a routine upgrade cycle for HRMIS to minimize the impact to the user community while optimizing new features and maintaining an up-to-date, supportable human resources management solution into the future.

In its continuing effort to improve and standardize the background check process outlined in the Guide to Judiciary Policy, Volume 12 (Human Resources), Chapter 5 (Employment), § 570 Background Checks and Investigations, the AO is pursuing a procurement for a new fingerprint solution that will standardize how all

[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/.

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 the security of the data, and improve the efficiency of the overall process. Unlike the legacy solutions, the new centrally maintained, web-based solution will operate on a local computer with other applications (i.e. JIFMS, JENIE) rather than on a stand-alone machine. No data will be stored on the local device, which will protect personally identifiable information (PII), and all data will be securely transmitted to a central repository.

The Ethics in Government Act requires all judicial officers and certain Judiciary employees to file financial disclosure reports. A new system for this purpose is in development, leveraging the executive branch tool and enhancing the functionality to meet the needs of Judiciary filers and those administering the program. Deployment has shifted and will begin in late FY 2020, with full deployment of the first phase in FY 2022. This new system is part of the larger program that includes correspondence automation and tracking; release and redaction; and compliance for financial disclosure reports.

Efforts are underway to develop and implement a COTS real estate and facilities management system to replace disparate systems and tools used today. The new system, called JSPACE, will provide comprehensive data and analytics for the Judiciary to manage more than 30 million usable square feet of space in 850 locations with an annual rental cost of almost $1 billion. Furthermore, it will support the Judiciary's long-range facilities planning efforts and overall rent and space management function as well as the Capital Security Program and initiatives such as space reduction and service validation. Full deployment is anticipated by FY 2023.

The AO is committed to improving emergency communications within the Judiciary. A new Judiciary Disaster and Recovery Tool (JDART) initiative began this year to provide improved information for assessing and monitoring a wide range of threats to Judiciary facilities and personnel. Based on current geographic information system technology, the new tool will provide a single operational view of developing emergency situations, e.g., natural or man-made disasters, and help Judiciary decision-makers and emergency personnel quickly and effectively assess and respond to evolving situations. The AO will also explore additional solutions to strengthen communications and situational awareness during emergency situations.

A standard set of development and integration platforms are being adopted within the administrative support arena. The platforms include low code, robotic process automation (RPA) with artificial intelligence (AI), service bus for application programming interface (API) centric integration, business intelligence and workflow solutions. The goal is to leverage these tools to reduce historical custom code complexity and replace it with standards-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 services and capabilities of these platforms will be incorporated in the service delivery model as the tools are adopted.

Coordinate and integrate national IT systems and applications from a Judiciary-wide perspective and more fully utilize local initiatives to improve services.

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 ready 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 developed in 2015. The plan, which is overseen by the AO Data Governance Board, identifies key activities, roles and responsibilities, and measures of success. It covers caseload, defender, finance and budget, human resources, probation and pretrial services, and space and facilities data. The plan's data vision is for the Judiciary to use data effectively in a consistent, reliable, and non-biased manner to inform decisions that are made to support its mission, including but not limited to the setting of policy and the allocation of resources. With input from the AO Data Governance Board, focus on achieving this vision over the last year has been on the following priorities:

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, and other relevant information) into a single interface, enabling powerful insights and enhanced analysis and reporting. In addition to the Court Unit Dashboard development, the Bankruptcy Caseload Explorer, the third and final product in the Caseload Explorer suite, was launched, providing Judiciary users greater accessibility and visibility to bankruptcy caseload data.

Enterprise business glossary: This will establish a common vocabulary and help communicate and govern the definition of business terms used within the AO. Through a collaborative approach involving data stakeholders from across the AO, work on developing definitions continued and drafting of an AO policy on use of the glossary began. To date, more than 150 definitions have been agreed to, with a focus on terms found in the Court Unit Dashboard.

Data literacy: This is defined by Gartner[4] as "the ability to read, write and communicate data in context" or "speaking data." Increasing data literacy throughout the Judiciary is essential as technological advances allow for both creation and consumption of an ever-increasing amount of data. 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 entered the procurement phase for the implementation of a new data governance and data management tool. This tool will help better catalog the Judiciary's data, set boundaries for the use of business glossaries and structured definitions, and continue efforts to develop data models for all current and planned data systems. A data model allows the business users to set the course for what data is included in a system and how it relates to all the other data in that system. These efforts 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.

Judiciary Data Working Group: The group was re-chartered in 2015 and three new judge positions were

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

added to include liaisons from three Judicial Conference committees that are significant stakeholders of data, including the Committees on Information Technology, Court Administration and Case Management, and Judicial Resources.

Data strategy and governance plan update: The current plan was developed in 2015 and, while much progress has been made, a refresh is needed to the approach and priorities. While many of the plan's goals have been met, fully or partially, others have not due to shifting priorities and resources. The AO has begun the process of working with stakeholders from across the AO to update the plan to reflect the current needs and priorities to drive the Judiciary's data governance and data literacy towards greater maturity.

More Fully Utilize Local Systems

Goals of the national IT program include developing and maintaining technology standards for local IT staff to ensure compatibility 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[5] developed by local courts have been supported nationally for several years and are used by many judges and chambers staff. In addition, a local application called Citation Links, which was already being used by 17 courts (see Judges and Chambers Staff section), has been 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 to support locally developed administrative applications continue. 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. The goal is to share the responsibility for implementing and supporting these critical functions and take advantage of the expertise that exists at the local courts and the AO. The Judiciary continues to look for similar opportunities.

To promote Judiciary-wide technical standards and enhance interoperability, a technical standards management process has been established. Technology best practices are also being identified to promote local or national applications having the greatest impact on court operations. 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.

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

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

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 stable, reliable national infrastructure that helps avoid 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 data center flexibility 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 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 public cloud providers, the WAN needs to become more dynamic and tuned to peak performance to maximize the use of low-cost circuits for lower priority applications. The SD-WAN will provide the Judiciary the ability to dynamically 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 network and server performance.

Enterprise Operations Center

The Judiciary has established an Enterprise Operations Center (EOC), which will provide 24/7/365 monitoring of the national infrastructure, services, and applications to identify IT issues before they impact end users. The EOC will support all national infrastructure and applications from one operations center and serve as the single service desk and interface for any incident related to national infrastructure and applications.

Over the next few years, the EOC will consolidate several disparate national IT support functions and provide central oversight of incident and problem resolutions. The EOC will go beyond 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 users.

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 cloud computing services in courts, including infrastructure and other hardware, database storage, computer applications, and server support. These services provide enhanced availability of Judiciary data and systems as well as an evolving catalog of cloud-

based solutions to the courts. These solutions can spur innovation, improve disaster recovery capabilities, and support a more mobile work force.

The design and implementation of a hybrid cloud will integrate the current on-premise Judiciary cloud with the best and most secure commercial offerings available. 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 impact, and other implications of cloud computing to provide guidance on these decisions. The overall benefit will be to increase the flexibility, 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.

Judiciary-wide guidelines for courtroom technologies serve as a baseline for the introduction of current and next-generation tools and capabilities. Research and proof-of-concept projects on technologies that will facilitate the efficiency of trials and hearings are ongoing and have included automated audio storage of court proceedings, networked audiovisual solutions, configured control systems (potentially replacing programmed control systems), cost reduction solutions, and training solutions. Improvements and efficiencies are being realized from digital video as well as 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.

Communications

In 2014, the Judiciary began the process of replacing its aging enterprise messaging system with a comprehensive, unified communications solution. The widespread adoption of mobile computing, document-sharing, and collaboration, as well as the dramatic shift in the market for messaging systems, necessitated this move. After developing high-level requirements and a cost estimate, migration options were evaluated, hosting decisions made, architectural engineering completed, and an implementation plan developed. The migration to this new system, which utilizes the Microsoft Office 365 platform, is complex and touches every Judiciary user and business process that utilizes email, instant messaging, word processing, spreadsheets, and collaboration tools. The deployment of the Microsoft Office 365 ProPlus software to all Judiciary users was completed by March 2019. The migration of all Lotus Notes Mail files to Microsoft Outlook was completed by January 2020.

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. AO staff identified requirements and configured the tool, developed governance and training, and established various support processes/services to support SPO implementation across the Judiciary. The AO has been working with court unit pilots since fall of 2018 and began a waved Judiciary-wide implementation in October 2019.

Deployment waves last a calendar quarter and were scheduled to be completed by July 2020. The SPO Center of Excellence provides governance/guidance, best practices, Judiciary use cases, and training schedules. The AO is assisting individual or groups of courts through opportunities and challenges and developing videos highlighting Judiciary/court type-specific use cases, tips and tricks, and demonstrations of important features.

Refine and update security practices to ensure the confidentiality, integrity, and availability of Judiciary-related records and information.

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 third annual Judiciary unit self-assessment period concluded in December 2019. Based on an analysis of data collected to date, including validations performed of 2018 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. The second annual national systems self-assessment period concluded in December 2019.

Mandatory independent court unit IT security assessments: This program launched in 2018. At least 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.

Increasing the use of the web application firewalls (WAF): To better protect internet-facing Judiciary web applications from malicious activity, the AO engages with courts and national program offices to help them understand how a WAF favorably differs from a traditional firewall. 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. Increasingly, courts are placing their CM/ECF applications behind the WAF to better protect them from malicious web traffic and external screen-scraping software that detrimentally affects the performance of court websites.

Judiciary Bug Bounty: Beginning in 2019, the AO has contracted a trusted firm to reward certain vetted third parties for information about any vulnerabilities or weaknesses they are able to identify in the Judiciary's public-facing infrastructure that could allow hackers to compromise Judiciary systems, applications or data. This program provides additional continual penetration testing against the Judiciary, resulting in valuable findings about real-world attack paths hackers could use. The AO validates these findings and provides detailed reports about them to courts and national program offices, complete with risk-mitigation recommendations.

Secure Socket Layer (SSL) decryption: Security devices monitor network traffic 24/7 with event logs aggregated and reviewed for evidence of malicious activity. The capability to inspect SSL traffic has been added to this process, which facilitates discovery of malicious activity that previously would have gone undetected. SSL decrypted traffic accounts for over 41 percent of all cyberattacks currently detected by the

Judiciary. The data gathered has enabled the Judiciary to proactively block attackers to prevent any disruption or degradation to essential services.

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 the main tool being utilized by the EOC to move toward proactively acting on identified issues before they impact the national infrastructure.

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.

Enhanced network segmentation: This 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, and 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 DCN resources.

Security infrastructure modernization for remote access: The Judiciary is assessing existing remote access services, products, and infrastructure for opportunities to enhance the remote access program, particularly for providing DCN access to a variety of devices. The Judiciary also is considering moving toward a Zero Trust Architecture, an information security model that requires verification for every user and device attempting to access an organization's network resources, regardless of how a device was furnished (e.g., by the Judiciary, personally owned, or other devices such as a hotel kiosk) and limits network resources to only those needed by the user.

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 notification, 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: National logging and firewall services deployed throughout the Judiciary generate a wealth of new information which the AO must analyze for threat indicators so that alerts are triggered and court notifications are sent in a timely manner. While additional data sources have been added from cloud environments and local court endpoints, existing technology suites still require improvements to their configuration and management to make their output 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.

Forensics: Digital forensic analysis is pivotal in determining the timeline and root causes of critical security incidents. Investments since last fiscal year 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 the hacker community, 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.

New security tools: Data from the Judiciary's cybersecurity efforts is continually analyzed to assess the need to modify or add tools to address vulnerabilities. As part of this effort, security solutions in the area of privileged account management are currently being deployed. A migration to a new endpoint protection tool is being planned for late calendar year 2020 to 2021. In addition, best practices are being developed regarding deployment of application "whitelisting" and file integrity monitoring tools. Licensing, hosting, training, and implementation strategies are being developed to effectively deploy these security tools.

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 additional facilities and systems to better 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. As indicated in this annual update to the Long Range Plan, not only will existing systems and infrastructure be maintained and enhanced, but emphasis will be placed on adopting new systems, technologies, and services that will provide additional benefits.

The table below shows the Judiciary's anticipated IT resource requests for fiscal years 2021 through 2025, organized by category within the Judiciary Information Technology Fund (JITF).[6] Successful execution of the objectives in this plan is dependent on the availability of funding. Each category is described in the next section.

Resource Requirements

	Current Estimate (Dollars in Millions)				
JITF Program Component	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**FY 2025**
Administrative and Management Systems	$75.7	$75.7	$107.5	$103.9	$105.4
Court Administration and Case Management	28.2	29.2	42.0	46.0	41.5
Court Allotments	106.3	104.0	107.4	109.0	109.7
Court Support	71.5	74.8	77.5	79.1	80.6
Infrastructure and Collaboration	135.7	135.8	160.0	164.0	180.7
Judicial Statistics and Reporting	17.1	17.2	24.2	24.4	24.7
Telecommunications	95.9	102.8	117.3	115.3	111.7
Subtotal	$530.4	$539.5	$635.9	$641.7	$654.3
Electronic Public Access Program	159.5	163.4	187.0	191.4	184.8
Total JITF Financial Requirements	$689.9	$702.9	$822.9	$833.1	$839.1

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

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.

Administrative Office of the U.S. Courts

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

www.uscourts.gov