Fiscal Year 2020 Update

Long Range Plan for Information Technology in the Federal Judiciary

Approved by the Judicial Conference of the United States

September 2019

Contents

Introduction

2020

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 not as something separate from their day-to-day work, but as a means by which they do their jobs. As business processes and information technology have become interwoven, the Judiciary recognizes that information technology presents opportunities not simply to replicate old paper processes in digital form but to rethink 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 information technology (IT) program over the next three to five years, and summarizes the Judiciary's anticipated IT resource requirements for fiscal years 2020 through 2024. 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. They were further informed by discussions within the AO's advisory process, as well as circuit judicial and IT conferences.

The *Long Range Plan* includes initiatives identified as part of a Judiciary-wide planning effort that began in fiscal year 2018. A group of Judiciary personnel that perform a wide variety of court and national IT functions first outlined IT themes critical to supporting the Judiciary's mission, then identified and refined initiatives that could be started over the next three years to achieve their desired results. As plans and cost estimates are developed, these new initiatives will continue to be added to the *Long Range Plan*.

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 information technology:

- 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.

Information technology 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 life cycle 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.

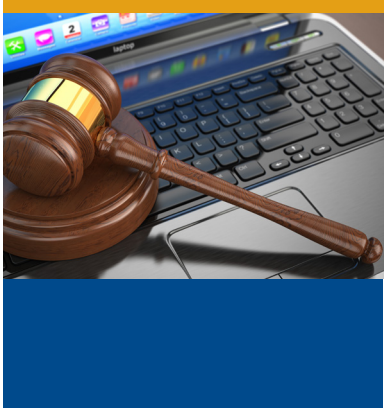
Electronic Public Access

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 the court in person to obtain a case file and photocopy documents. Instead, the program's two 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 is establishing a Public User Group to allow for the exchange of information regarding public access issues experienced by the PACER user population as well as recommend ideas for expanding and improving services and the user experience. The EPA program is also working to modernize the PACER user interface. Work continues on updating the public-facing applications accessible from the PACER website 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 perform their job with a minimum of keystrokes. 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 primarily implement security updates, but will also address any necessary changes (due to new rules, for example). These annual NextGen releases will also include security upgrades as well as new functionality and re-written modules, based on priorities established by court expert panels.

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 supervisory and investigatory tool that enables officers to carry larger caseloads with fewer support staff. While this application has greatly served the probation and pretrial services community, the Judiciary is moving toward identifying a replacement that will be workflow-based, improve performance and stability, and rapidly deliver new

business functionality to the user community. 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. Pre-solicitation activities, including a data migration strategy, will continue through mid-fiscal year (FY) 2019. Solicitation and contract award will follow.

As a replacement system is developed, other probation and pretrial applications that work with PACTS will be assessed for inclusion in the new system. Applications that are not appropriate for inclusion will undergo additional assessment to determine whether they should be retired, redesigned, or updated. During this assessment and review process, investment in the legacy applications will continue so that business needs are met and stability is maintained.

The mobile version of PACTS (iPACTS) provides probation and pretrial services officers across the country access to caseload information as well as email and the Judiciary's intranet sites from their mobile devices. The replacement system is expected to increase mobile functionality, expanding the availability of caseload information both on- and offline.

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 using a new 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 a proof of concept in 2018 with five district and bankruptcy courts. Features will include the ability to create and manage case-related entries (e.g., hearings, trials, and documents associated with the case), as well as non-case related calendar entries (e.g., vacations). The calendar will also allow management of calendar-related resources such as courtrooms, staff, and equipment. Once the calendar pilot period ends, wider release will be determined.

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. JIFMS provides enhanced interfaces with external systems, improved data sharing capabilities, improved internal controls, and standardized business practices. Leveraging a single system for these functions helps strengthen application security, allowing for more efficient system upgrades, and reduces maintenance requirements. JIFMS implementation will serve as a springboard to introduce new capabilities to improve and streamline financial management functions throughout the Judiciary.

Efforts are now focused on replacing the Civil/ Criminal Accounting Module, which supports the civil and criminal debt management function within the district courts. Implementation activities started in 2018 and are expected to be completed in 2020. Development efforts are also underway for an automated collection and receipting system to replace the various systems used by district, bankruptcy, and appellate courts. The solution is being designed to integrate with the Judiciary's financial and case management systems.

The Human Resources Management Information System (HRMIS) manages human resources transactions, including leave tracking and employee performance management, and produces payroll for the Judiciary. Planned system improvements focus on reducing costs and streamlining human resource management processes. Reporting and leave tracking functions will also be enhanced to enable data sharing among systems and to expand mobile offerings.

The Ethics in Government Act requires all judicial officers and certain judicial employees to file financial disclosure reports. A new system for this purpose is in development, leveraging the system being used in the Executive Branch, and will enhance functionality to better meet the needs of filers and those administering the program. Deployment is planned to begin in FY 2019, with full deployment in FY 2020.

Changes are also on the horizon for the Judiciary's facilities management systems. A commercial off-the-shelf real estate and facilities management system will replace disparate systems and tools. The new system will provide the 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 2021.

Efforts are underway to adopt a standard set of development and integration platforms within the administrative support arena. The goal is to reduce the complexity of the IT environment, enhance security, improve quality, provide consumer friendly solutions, and reduce the time to market for administrative support products and services.

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.

A data strategy and governance plan guides the Judiciary's efforts to manage data as an enterprise asset. Overseen by a Data Governance Board, the plan 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. Achieving the plan will afford the federal Judiciary better decisions and reduced costs associated with data collection, management, and analysis as well as a reduced burden on Judiciary personnel, allowing them to do their jobs more effectively and efficiently. The AO Data Governance Board has approved five major initiatives aimed at

furthering the strategic approach to managing data as an enterprise asset. Achieving these priorities will facilitate a more systematic way of sharing data between systems, replacing individual system-to-system definitions and agreements.

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 representatives from the AO and various court units, an initial group of definitions has been completed, with a second group in progress. These will be communicated throughout the Judiciary, including notations and links to relevant documents in the *Guide to Judiciary Policy*.

Enterprise conceptual data model: The conceptual data model provides an overview of the high-level data categories and their relationships. It consists of data domains--or subject areas--that include case, judge, human resources, finance and budget, probation and pretrial, and space and facilities. It is being developed through an analysis of existing documents and data gathered for the enterprise business glossary, informed by subject matter experts.

Enterprise data lineage model: This maps the creation, movement, transformation, use, and storage of data. Diagrams of more than 250 Court Profile and caseload terms from Judiciary statistical sources and reports have been created. This effort will be expanded to include administrative and other systems to create an enterprise data flow model.

Enterprise data asset inventory: The inventory identifies existing systems, databases, tables, reports, and publications and how they are used, including the database, table, and business element names and definitions. This effort also has begun using caseload terms and data assets and will be expanded over time to include enterprise-wide data.

Enterprise policy and process initiative: This identifies existing and required guidelines necessary to enable or restrict usage and access to particular data, and to define data and naming standards. This effort is currently focused on the operations, processes, communication, and collaboration within the Data Governance Board and between the board and the various system and data owners.

Efforts to make data available between courts in a more seamless, dynamic, and interactive manner are underway. A demonstration project, aimed at making court information available to 17 participating courts through an easy-to-use dashboard, is in progress. Information is drawn from caseload, space and facilities, and human resources data, with participating courts agreeing to make their data available to each other.

The Judiciary is also working to make more interactive data available to the general public. Historically, statistical data were published through static, printed reports. During the past decade, statistical reports were made available in PDF on www.uscourts.gov, which expedited the release of data and saved money on printing reports. Many of the data files have now also been made available on the website in downloadable Microsoft Excel format, which saves users accessing multiple tables in different reports significant time and effort. Moreover, the Judiciary has launched an initiative to provide the public even more seamless, dynamic access to this data using analytics software such as data visualization tools. This will allow both novice and more advanced users to explore or download data and to build their own data tables, charts, and graphs.

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 developed by local courts have been supported nationally for several years and are used by hundreds of 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.

The CASE dashboard is a web-based tool available for all devices (e.g., tablets and mobile phones) developed locally to enhance data management efforts. Developed by the District of Connecticut, it displays real-time information from various case and jury management systems. It has views for pending cases, case trends, and judge and law clerk assignments, in addition to providing reports, emails, and contact information. The dashboard can be easily and quickly configured for a specific judge. The court is planning to release the platform for creating judge-specific dashboards to interested district courts and is also working to create a bankruptcy court version of the tool.

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 avoidances. The Judiciary's reliance on information technology 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, be tuned to peak performance, and 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 set the stage for 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. This effort will begin by establishing a proof-of-concept commercial cloud to evaluate and document expected cloud use cases. It will then be followed by acquisition of commercial cloud services that 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 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 audio retrieval, evidence displays for jurors, and expanded wireless capabilities. Improvements and efficiencies are being realized from digital video as well as centralization of audio platforms and videoconferencing systems. Rapid changes in the audiovisual industry have changed the way technologies are implemented within the courtroom, 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 first migration effort focused on implementing software for desktop tools, with email migration targeted for completion by 2020.

The communications platform also includes the collaboration tool, SharePoint, which integrates with Microsoft Office 365 and contains capabilities previously not available to the Judiciary in a single platform.

Plans are being made to unlock the potential of this tool across the Judiciary while protecting and securing the information it contains. Priorities identified in a nationwide planning session include strategy; roles and governance; integration with national systems; enterprise search capabilities; collaboration with external entities; deployment, migration, acceptance, and adoption; training and support; and secure and mobile access.

Business requirements and an implementation plan have been developed for national and local use. Eight court units across seven pilots (including one pilot with two court units that share administrative services) are participating in a proof of concept to test such things as migrations, integration with Office 365, use with Mac-based technology, and enterprise search parameters. Guidance on local governance and administration options is being provided, as are training and communications materials. A phased implementation is anticipated, beginning in the fall of 2019.

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 multiple layers of defenses which are designed to protect networks and information through preventive measures. Network and host-based systems are employed to routinely inspect traffic for signs of malicious activity which can be blocked or alerted for analysis. Breaches of Judiciary networks or data are also prevented by 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, network access controls, endpoint protection systems, encryption solutions, and patch management solutions. Identity management and authentication systems enforce access rights to Judiciary data, and web-based threat protection systems prevent end user access to known malicious sites on the internet. Finally, security testing and assessments proactively identify vulnerabilities for corrective action before they can be exploited. Efforts receiving focus over the next three to five years include the following:

Annual IT security self-assessments: Each court unit 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 will evolve over time in an effort to incrementally improve the security baseline and to address emerging threats. The second annual self-assessment period concluded in December 2018. Based on an analysis of data collected to date, including validations performed of 2017 results during the mandatory independent court unit IT assessments, minor refinements to the self-assessment have been made for the upcoming self-assessment period. Building on the success of this initiative, it has been extended in 2018 to include assessment of the effectiveness and maturity of security programs supporting national applications, such as case management (CM/ECF and PACTS), financial management (JIFMS), and identity management.

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.

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.

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 developed a roadmap to implement additional capabilities of these firewalls, such as vulnerability protection, spyware, and antivirus blocks, as well as URL filtering, which controls access to known hostile websites.

Secure Socket Layer (SSL) decryption: Security devices monitor network traffic 24 hours a day, 7 days a week, 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 nearly 30 percent of all cyber-attacks currently targeting the Judiciary. The data gathered has enabled the Judiciary to proactively block attackers to prevent any disruption or degradation to essential services.

Enhanced network segmentation: This will enhance the DCN by restricting access to specific network segments based on the health and location of the device connecting to it, enabling limited network access. This can be done at the local court local area network (LAN) level as well as at the national data centers.

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.

Detecting, Analyzing, and Mitigating Intrusions

Activities in this area allow the Judiciary to react quickly and effectively to suspected security incidents. It includes analyzing indicators of malicious activity detected by the mechanisms previously described, including event notification, remediation support, and data forensics. It also includes event correlation and analysis of activities across multiple services, tools, and devices. Furthermore, 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. Ongoing evaluation of cyber threat trends and their potential impact on Judiciary assets as well as incorporating data derived from new tools is necessary to keep these capabilities current. Efforts in this area will include the following:

Log management, analysis, and notification: National logging and firewall services being deployed throughout the Judiciary are generating a wealth of new information which must be analyzed for threat conditions so that alerts are triggered and court notifications are sent in a timely manner. Existing technology suites require expansion to process and glean value from these large data sets.

Data management: The Judiciary will seek ways to more effectively collect and analyze information,

such as data visualization and risk management tools to effectively translate data into actionable information. Within the national IT security program, for example, results from the annual court unit IT security self-assessments utilized these tools to provide data about the impact of national IT security investments on security baselines as well as areas in which documentation supporting the self-assessment process needed to be strengthened.

Forensics: Digital forensic analysis has been pivotal in determining the timeline and root causes of critical security incidents. Initial investments 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. Additional investments are being pursued to further strengthen these capabilities and improve overall collection reliability and response time.

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. At present, red team services continuously assess the overall security posture of the AO's network, systems, and users at its disparate locations. In limited proofs of concept, volunteer courts validated the usefulness of this service outside of the AO, which has generated demand for additional red team engagements. The availability of this service across the Judiciary will be dependent on the level of funding available.

Shaping the Cybersecurity Environment

The Judiciary is focused on creating and maintaining 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 need policies, tools, information, and education required to perform their respective roles. New efforts over the next three to five years include the following:

Court and defender services data networks: Coordination between the courts and defender communities, which each have their own data networks, has resulted in agreements to ensure cybersecurity risks are proactively managed at the interconnection between these networks and that prohibited traffic will be blocked.

IT security education: An IT security training curriculum will provide all IT personnel awareness and expertise on security topics and techniques that are vital to a secure Judiciary. This program launched in 2017, and includes a curriculum providing a deep understanding of foundational security elements that need to be understood, implemented, and maintained by court IT specialists across the Judiciary. The curriculum will be expanded to include network fundamentals and advanced security practitioner classes along with training on national applications that focus on cybersecurity principles. Additional learning opportunities will be created for court unit executives and judges on this critical topic.

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 areas of privileged account management, endpoint protection, file integrity monitoring, and application "whitelisting," are underway. Licensing, hosting, training, and implementation strategies are being developed to prioritize procurements and effectively deploy security tools.

Cyber threat intelligence: Open-source intelligence collection and analysis strengthens the national IT security program by identifying new vulnerabilities, detecting imminent threats, developing attack trends and 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 to integrate into the executive branch clearance management process will allow the Judiciary to incorporate classified data into emerging analytic efforts.

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 2020 through 2024, organized by category within the Judiciary Information Technology Fund (JITF).[2] 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 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**
Administrative and Management Systems	$74.9	$74.3	$84.4	$83.7	$83.7
Court Administration and Case Management	34.1	30.7	42.9	44.3	47.2
Court Allotments	99.8	106.3	111.1	111.5	113.1
Court Support	65.6	67.8	71.2	72.6	74.1
Infrastructure and Collaboration	152.5	137.3	159.1	161.2	162.4
Judicial Statistics and Reporting	16.9	17.7	25.3	25.4	25.5
Telecommunications	93.7	96.3	136.2	120.7	117.8
Subtotal	$537.5	$530.5	$630.2	$619.4	$623.8
Electronic Public Access Program	175.1	178.9	184.6	185.8	182.2
Total JITF Financial Requirements	$712.6	$709.4	$814.8	$805.2	$806.0

[2] 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 facilities projects and travel expenses and Judiciary websites.

Court Administration and Case Management

This category includes 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; and 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. This includes 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 security associated with the Judiciary's full enterprise hosting and cloud computing services and email and collaboration systems. It also includes the costs of infrastructure for new courthouse construction projects and IT 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 it 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