

Fiscal Year 2018 Update

Long Range Plan for Information Technology in the Federal Judiciary



Approved by the Judicial Conference
of the United States

September 2017

Contents



Introduction	1
Strategic Priorities.....	2
Continue to build and maintain robust and flexible technology systems and applications.....	2
Coordinate and integrate national IT systems and applications.....	5
Develop system-wide approaches to the utilization of technology	7
Refine and update security practices.....	8
Investing in the IT Program.....	12
Resource Requirements.....	12
JITF Program Components.....	13

Introduction

2018

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 has also come to recognize 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 transmits 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 2018 through 2022. 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. They were further informed by discussions across the Judiciary by focus groups, the AO's advisory process, and 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 is comprised 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, upgrade, 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, in order 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 program is working to modernize the PACER user interface. In addition, the PACER Case Locator is being updated to include new features. These include a simplified search option with advanced search capabilities; breadcrumbs for improved navigation; the ability to bookmark cases, save frequently used searches, and set a preferred landing page; and displaying pages properly on any device including tablets and mobile devices.

Case filing/case management

The filing process in the federal courts 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) will modernize the business processes used by the courts and judges' chambers. NextGen will enhance the way judges manage case information, providing the information they need to perform their job with a minimum of keystrokes. Another major benefit to NextGen is that it will enable judges, court staff, and attorneys to access CM/ECF data in multiple courts using a single account. Functionality is also being developed that will allow appellate judges to export case documents to a mobile device.

NextGen will also improve filing capabilities for pro se filers in bankruptcy cases, enhance the Judiciary's ability to exchange data within its internal systems and between internal and external systems, and support a more consistent user experience for external users of the case management system.

The first release to appellate courts was finalized in the fall of 2015. Currently ten courts are using the NextGen application. Seven district and bankruptcy courts are also using the software as part of the pilot process to provide feedback for improvements to the applications. The goal is to make the release available to all courts by 2018.

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 system will be workflow based, improve performance and stability, and have the



ability to 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.

The mobile version of PACTS (iPACTS) has provided access to caseload information to probation and pretrial services officers across the country with tablet and laptop computers, as well as software that gives officers access to key case information, email, and the Judiciary's intranet sites from their mobile devices.

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 users with the ability to automatically create and maintain electronic packets of information for matters that require chamber's review and actions. The bankruptcy case openings module will store data elements in a series of electronic forms from which data is extracted and entered into CM/ECF automatically. Central Sign-On allows each user a common username and password to be used for all courts that adopt NextGen CM/ECF. Judges and their staff will also have the advantage of using a new user interface called Workspace, which provides customizable screen content based on their job function. Mobile Briefcase is the newest feature and allows appellate judges to download and edit documents on a tablet computer. Additional enhancements will continue to be evaluated and prioritized in future releases of NextGen.

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 and secure administrative solutions.

The financial management system currently used by the courts is in the process of being upgraded to the Judiciary Integrated Financial Management System (JIFMS). This will result in a single financial application supporting the Judiciary's core accounting

and procurement function and is scheduled for completion by the end of calendar year 2017. JIFMS will provide enhanced interfaces with external systems, improved data sharing capabilities, improved internal controls, and standardized business practices, which will also strengthen application security, allow for more efficient system upgrades, and reduce maintenance requirements.

Following the deployment of the core accounting and procurement functions, plans are in place to replace the Civil/Criminal Accounting Module, which supports the civil and criminal debt management function within the district courts. Development will commence in late 2017 with implementation targeted to begin in 2018. Planning is also underway for an automated collection and receipting system to replace the various systems used by district, bankruptcy, and appellate courts, and will be integrated with JIFMS.

The Human Resources Management Information System (HRMIS) manages human resources transactions, including leave tracking and employee performance management, and produces payroll for the Judiciary. The system's application software and tools were recently upgraded, which will provide a more secure platform. Planned system improvements focus on reducing costs and streamlining human resource management processes. For example, a module which will allow human resources professionals to complete employee suitability requests electronically and monitor the status of those requests will be implemented later in 2017. This will reduce the number of manual requests, increase the visibility of each request at the local court/unit, and streamline a labor-intensive manual process. Also in progress is an effort to streamline the on-boarding process for employees and contractors. This will expedite the provisioning of services and accounts and reduce redundant data entry into multiple systems. Finally, reporting and leave tracking functions will 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 will be deployed in fiscal year 2018 to support the 2017 reporting cycle and will enhance functionality to better meet the needs of filers and those administering the program.

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. It 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. It will support the Judiciary's long-range facilities planning efforts and overall rent and space management function as well as initiatives such as space reduction, service validation, and the Capital Security Program. Full deployment is anticipated by fiscal year 2021.

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. The Judiciary will benefit both technically and programmatically by further 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 number of techniques and technologies provide opportunities for the Judiciary to integrate its national systems and manage information from an enterprise-wide perspective. Technologies such as web services and service-oriented architecture for use in national systems have moved the Judiciary forward in this area.

A data strategy and governance plan has been created and will be implemented over the next three years. With goals focused on leadership and culture, data governance, data architecture and security, and data reporting and analysis, 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. Key activities include developing an enterprise-wide data dictionary and enterprise data architecture, reaching clarity on key terms and definitions that cross programs, improving data quality, modernizing approaches to data access and visibility, and developing enhanced data analytics to better inform decision making. 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.

In early 2017, the AO Data Governance Board approved five major priorities for the next several years. They are aimed at improving the strategic approach to managing data as an enterprise asset and involve developing the following: (a) an enterprise business glossary providing consistent definitions of terms; (b) an enterprise conceptual data model that identifies existing data and relationships; (c) an enterprise information flow model that identifies the location and source of data; (d) an enterprise data asset inventory that identifies existing reports, tables,





and publications and how they are used; and (e) an enterprise policy and process initiative to identify existing and required guidelines necessary to enable or restrict usage and access to particular data. Achieving these priorities will facilitate a more systematic way of sharing data between systems, replacing individual system-to-system definitions and agreements.

Additionally, the Judiciary is working to make more interactive data available to the general public. Historically, statistical data were published on an annual and/or quarterly basis through static, printed reports. During the past decade, to expedite the release of data and save money spent on printing reports, statistical reports began to be made available in their traditional layouts in PDF format on www.uscourts.gov. Recently, many of the data files were made available on the website in downloadable Microsoft Excel format; users accessing multiple tables in different reports expend significant time and effort in doing so. The Judiciary has launched an initiative to provide the general public more seamless, dynamic access to this data in addition to providing it in Microsoft Excel format. Emerging analytics software (such as data visualization tools) 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

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 providing

national support. 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. 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, the NextGen CM/ECF initiative has included a local application called Citation Links which was already being used by 17 courts. By including this functionality in NextGen, not only will it be available to all courts, but the support burden on the local court will be alleviated. This model of incorporating valuable local developments into national systems will continue to be applied in the future.

Efforts are also underway to leverage the national systems infrastructure to support locally developed administrative applications. 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 these critical functions and take advantage of the expertise that exists at the local courts and the AO. Both systems have taken advantage of AO services to ensure that the architectural, security, and management requirements of a national application are addressed. Both have transitioned Tier 1 help desk services to the AO and have started to leverage the AO's testing and training services.

To promote Judiciary-wide technology standards and enhance interoperability, a technology standard process has been established to develop an enterprise architecture. 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. It will also link to enterprise guidance and best practices on deployed technologies and help identify local applications that are candidates for national support.

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 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 Wide Area Network Diversity project, designed to increase the overall network availability and reliability through carrier diversity and redundant connections, is nearing completion.

A new initiative on the horizon is Intelligent Wide Area Network (IWAN), 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, the WAN can be tuned to peak performance or to reduce cost by maximizing the use of low cost circuits for lower priority applications. The IWAN will provide the Judiciary the ability to dynamically route, monitor, and measure real-time traffic in order to optimize performance.

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 an evolving catalog of cloud-based solutions to the courts and enhanced availability of Judiciary data and systems. Access to these solutions can spur innovation, improve disaster recovery capabilities, and set the stage for a more mobile work force. These services will be provided through the design and implementation of a hybrid cloud which integrates the current on-premises Judiciary cloud with the best and most secure commercial offerings available.

Courtroom technologies

In the courtroom, the Judiciary has made substantial investments in 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 and 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 developing a plan to replace 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 will be complex and is expected to take approximately four years to complete, including decommissioning the existing infrastructure following implementation in the courts.

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 data communication network, its underlying infrastructure, and the applications that serve its mission, is 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 gain, or simply to cause embarrassment, and are continually 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 establishes and implements the national security architecture, provides several security assessment and testing services, and conducts risk-based planning, among other activities. It encourages court units to implement analogous concepts within their environments through the use of network segmentation techniques, security policies, privilege management, and related activities. 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 data communications network (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 will assess the effectiveness and maturity of its local IT security program using a common rubric. Results will be 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 to address emerging threats. The first annual self-assessment period will conclude in December 2017, with the program continuing to evolve thereafter.

National logging service: This centrally-managed service will enable 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 begun an effort to install 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. This will ensure a consistent configuration across locations and complements the security infrastructure at the Judiciary data centers. Upon completion of the deployment, the Judiciary will leverage additional firewall capabilities, such as intrusion prevention, which monitors the network for malicious activity, and URL filtering, which controls access to known hostile websites.

Mandatory independent court unit IT security assessments: At least once every five years, each court unit will

receive a comprehensive independent assessment of its management, technical, and operational safeguards to understand their safeguard strengths and weaknesses. They will also receive feedback on the efficacy of the self-assessment program within their court unit. The program is anticipated to begin in 2018.

Secure Socket Layer (SSL) decryption: Security devices already monitor network traffic 24 hours a day, seven 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. Full deployment of this capability will be completed in 2017, with ongoing analytic support in subsequent years.

Penetration testing: Using tactics commonly employed by the hacker community, penetration testing validates network defenses by identifying vulnerabilities and enabling continuous improvement. Initial activities will focus on the AO, with rules of engagement to be developed before expanding to the court community.

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. Activities also 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 in order 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 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.

Forensics: These tools and related training will allow the Judiciary to analyze security incidents, determine their impact and root causes, and remediate risks.

Shaping the cybersecurity environment

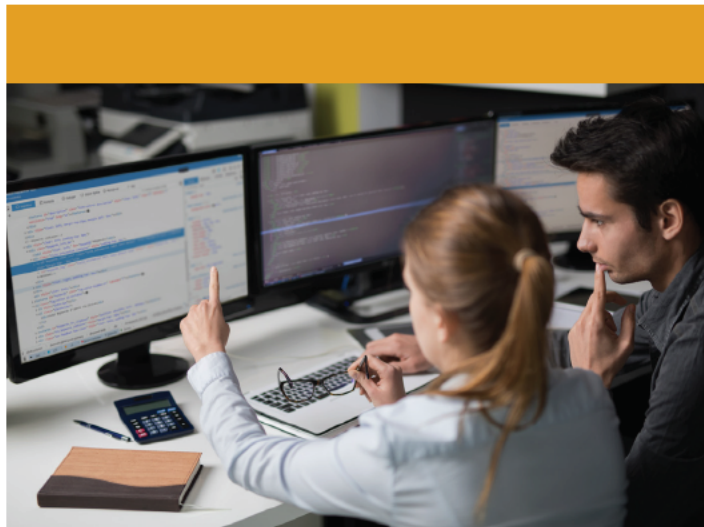
The Judiciary is focused on creating and maintaining a security-aware culture using recognized best practices for information security. Development and oversight of the *Judiciary Information Security Framework* (Framework) provides the foundation to effectively manage risks, make informed decisions 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, is underway to ensure cybersecurity risks are proactively managed at the interconnection between these networks. Analysis will be complete in 2017 and will determine the type of technical enforcement to be implemented.

IT security education: An IT security training curriculum will provide all IT personnel awareness and expertise on security topics and techniques that are foundational 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 continue to evolve with the program, and additional learning opportunities will be created for court unit executives and judges on this critical topic.

New security tools: An independent study was concluded in late 2016 to identify security solutions to assist in the areas of privileged account management, file integrity monitoring, application “whitelisting,” patch and asset management, endpoint forensics, and web-based threat protection. Associated licensing, hosting, training, and implementation strategies are being developed in order to prioritize associated procurements and effectively deploy these tools.



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 in 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 systems in place be maintained and enhanced, but emphasis will also be placed on adopting new systems, technologies, and services that will provide additional benefits.

The table shows the Judiciary's anticipated IT resource requests for fiscal years 2018 through 2022, 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 2018	FY 2019	FY 2020	FY 2021	FY 2022
Administrative and Management Systems	\$81.2	\$77.4	\$73.8	\$68.3	\$70.9
Court Administration and Case Management	38.2	38.8	30.3	30.9	31.2
Court Allotments	90.6	83.3	89.1	90.8	92.9
Court Support	54.1	55.0	56.3	57.3	58.6
Infrastructure and Collaboration	166.3	152.8	156.2	159.1	157.8
Judicial Statistics and Reporting	21.4	17.0	25.6	26.2	26.9
Telecommunications	83.1	82.3	96.8	105.4	110.3
<i>Subtotal</i>	\$534.9	\$506.6	\$528.1	\$538.0	\$548.6
Electronic Public Access Program	161.9	187.9	197.9	203.4	185.9
<i>Total JITF Financial Requirements</i>	\$696.8	\$694.5	\$726.0	\$741.4	\$734.5

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, travel expenses, and Judiciary websites.

Court administration and case management

This category encompasses the probation and pretrial services personnel case management system. Also included are tools to access critical case information and law enforcement databases; systems for juror qualification, management, and payment; and the system that captures requests for payments to private court-appointed counsel and expert service providers.

Court allotments

These allotted funds cover costs paid directly by the courts for operating, maintaining, and replacing computers, printers, local-area-network equipment, and software. Also included in this category are costs for local telecommunications services, equipment, and maintenance.

Court support

This category funds staff that provides 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 the building and maintenance of 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 IT systems support, maintenance, testing, 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 provides support for voice, data, and video transmission services and telecommunications. The Judiciary's communications program allows the Judiciary to operate communications services for the appellate, district, and bankruptcy courts and for probation and pretrial services offices, as well as 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