JUDICIARY INFORMATION TECHNOLOGY FUND

GENERAL STATEMENT AND INFORMATION

The Judiciary Information Technology Fund (JITF) was established by Congress in fiscal year (FY) 1990 (28 U.S.C. § 612) to assist the judiciary in implementing its information technology (IT) initiatives. The JITF authority was extended indefinitely in the FY 1998 Commerce, Justice, State, Judiciary, and Related Agencies Appropriations Act (P.L. 105-119). The JITF was authorized "without fiscal year limitation" for the procurement of IT resources. The JITF makes it possible to manage the IT program over a multi-year planning cycle, allowing for more effective and efficient planning and budgeting for IT activities.

In keeping with the judiciary's mission and primary business objectives, the IT program must identify, implement, and maintain cost- effective solutions for the judiciary, bar, and the public. All IT expenses for the appellate, district, and bankruptcy courts and for probation and pretrial services offices must be paid from the JITF.

JITF requirements are financed from a variety of sources:

- deposits from the courts' Salaries and Expenses (S&E) account;
- fee collections from the Electronic Public Access program for IT expenses specifically related to improving public access to court information (see Appendix 2, EPA for more information on this program);
- unobligated balances from prior year financial plan savings (unencumbered);
- proceeds from the sale of excess IT equipment;
- annual allotments to the courts originally for non-IT purposes that are reprogrammed locally by the courts for IT initiatives, in accordance with the judiciary's budget decentralization process; and
- deposits from other judiciary appropriations that are non-mandatory judiciary users of the JITF (such as the Court of Appeals for the Federal Circuit (CAFC), the Court of International Trade (CIT), the U.S. Sentencing Commission (USSC), Court Security, the Federal Judicial Center (FJC), and the Administrative Office of the U.S. Courts (AO)).

The majority of financing in the JITF originates from deposits from the S&E account. Table 11.1 below displays JITF requirements and funding sources for FY 2025 through the FY 2027 request. Tables 11.2 and 11.3 provide additional data about obligations and outlays.

Table 11.1 JITF Obligations and Financing ($000)

Description	FY 2025 Actual	FY 2026 Plan	FY 2027 Request
Financing:			
Salaries and Expenses			
Unobligated Balance, Start of Year	152,164	31,799	20,000
New Deposits and Prior Year Recoveries	568,670	733,182	790,724
Unobligated Balance, End of Year	(31,799)	(20,000)	-
Total Salaries & Expenses	**689,034**	**744,981**	**810,724**
EPA Program			
Unobligated Balance, Start of Year	161,987	166,584	76,825
Estimated Receipts and Prior Year Recoveries	172,233	157,000	157,000
Unobligated Balance, End of Year	(166,584)	(76,825)	-
Total EPA Program	**167,636**	**246,759**	**233,825**
Administrative Office of the U.S. Courts			
Unobligated Balance, Start of Year	2,872	3,938	-
New Deposits and Prior Year Recoveries	3,594	-	-
Unobligated Balance, End of Year	(3,938)	-	-
Total Administrative Office of the U.S. Courts	**2,529**	**3,938**	**-**

Description	FY 25 Actual	FY 26 Plan	FY 27 Request
Court of Appeals for the Federal Circuit			
Unobligated Balance, Start of Year	3,443	4,138	3,346
New Deposits and Prior Year Recoveries	2,615	1,071	1,818
Unobligated Balance, End of Year	(4,138)	(3,346)	(2,542)
Total Court of Appeals for the Federal Circuit (Non- EPA)	**1,920**	**1,863**	**2,622**
Court of International Trade			
Unobligated Balance, Start of Year	1,488	1,083	100
New Deposits and Prior Year Recoveries	448	-	-
Unobligated Balance, End of Year	(1,083)	(100)	-
Total Court of International Trade (Non- EPA)	**852**	**983**	**100**
Federal Judicial Center			
Unobligated Balance, Start of Year	949	949	323
New Deposits and Prior Year Recoveries	-	-	-
Unobligated Balance, End of Year	(949)	(323)	(323)
Total Federal Judicial Center	**-**	**626**	**-**
U.S. Sentencing Commission			
Unobligated Balance, Start of Year	1,844	1,721	-
New Deposits and Prior Year Recoveries	200	-	-
Unobligated Balance, End of Year	(1,721)	-	-
Total U.S. Sentencing Commission	322	1,721	-
GRAND TOTAL JITF	**862,293**	**1,000,872**	**1,047,271**

Table 11.2 Obligations by Budget Object Class ($000)

Description	FY 2025 Actual	FY 2026 Plan	FY 2027 Request
21.0 Travel and Transportation of Persons	4,588	5,325	5,572
23.3 Communications, Utilities, and Misc. Charges	38,049	44,164	46,210
24.0 Printing and Reproduction	5,201	6,037	6,317
25.1 Advisory and Assistance Services	360,019	417,878	437,237
25.3 Other Goods and Services from Federal Sources	121,897	141,487	148,042
25.7 Operation and Maintenance of Equipment	53,019	61,540	64,391
26.0 Supplies and Materials	6,666	7,737	8,096
31.0 Equipment	272,854	316,704	331,376
Total Obligations	**862,293**	**1,000,872**	**1,047,239**

Table 11.3 JITF Relation of Obligations to Outlays ($000)

	FY 2025 Actual	FY 2026 Plan	FY 2027 Request
Direct Obligations Incurred	862,293	1,000,872	1,047,271
Obligated Balance, Start of Year	541,612	482,737	654,520
Adjustments of Prior Year Activity	(74,991)	-	-
Obligated Balance, End of Year	(482,737)	(654,520)	(806,174)
Total Outlays	**846,177**	**829,089**	**895,617**
Less Offsets	(205)	-	-
Net Outlays	845,972	829,089	895,617

PROGRAMS FUNDED FROM THE S&E ACCOUNT

Under the guidance of the Judicial Conference of the United States and according to the strategic direction and objectives contained in the *Long-Range Plan for Information Technology in the Federal Judiciary*, the judiciary continues to implement IT systems to meet the mission of the courts. The judiciary, like the rest of the public sector, depends on technology for communication systems, research, and information management systems to fulfill mission-critical needs.

The judiciary has a successful enterprise-wide IT program upon which judges, court staff, probation and pretrial services officers, and others depend to conduct their mission-critical functions. This program includes a vital data communications infrastructure that connects all court units securely and is the lifeline for information transfer, applications that ensure the judiciary manages its resources effectively, and various court support projects and case management systems that provide judges and staff the tools they need to perform their day-to-day work.

Judges and chambers staff rely on IT equipment, software, and complex data communication networks through which they access electronic case management systems, email, legal research databases, and numerous websites and applications. Many courtrooms are equipped with technologies that improve the quality and efficiency of courtroom proceedings through reduced trial time and improved fact-finding. A variety of IT tools help judges do their work more efficiently in areas ranging from text-search capability across pleadings, opinions, and court records to the timely receipt of critical information through seamless transmission of data from one court type to another.

SIGNIFICANT ACTIVITIES

Cybersecurity and IT Modernization Efforts

The combination of cyberattacks on judiciary IT systems and aging legacy applications critical to court operations has created IT vulnerabilities that require additional resources. The judiciary is working to address these IT vulnerabilities and strengthen the judiciary's ability to provide core IT services and cyber protections for the courts. Cybersecurity and IT modernization are identified as strategic priorities in the *Long-Range Plan for Information Technology in the Federal Judiciary* because they ensure that the judiciary can continuously improve and secure judiciary-related records.

The judiciary developed a multiyear *Cybersecurity and IT Modernization Strategy* (*Strategy*) to address the actions and initiatives necessary to respond to aging critical hardware, applications with outdated and potentially insecure software, and overburdened staff. The *Strategy* provides a framework to support changes needed in judiciary IT governance, the establishment of enterprise standards, improvements to enterprise visibility, and modernization of the security of systems and solutions across the judiciary. The *Strategy* also positions the judiciary to be ready for technological advances.

Activities outlined in the Strategy include:

- Increasing IT standardization throughout the branch to improve the security of IT networks and systems by ensuring local court IT systems and solutions are compatible with national applications and security requirements;
- Modernizing the Enterprise Data Warehouse (EDW) by moving from its current platform, which is built on outdated technology, to a new cloud-based platform with enhanced data management services;
- Replacing the judiciary's legacy system for identity management with a modern identity, credential, and access management system; and
- Improving and enhancing the technical and operational capabilities of the judiciary by securing the judiciary's IT environment, personnel, equipment, and systems from cyber threats.

The judiciary has made significant progress on the requirements outlined within the Strategy. To date, two of the ten initiatives, Data Center Move and Unified Communication, have been completed. Several projects within the eight other initiatives have also been

completed, each strengthening the judiciary's security posture by enhancing its ability to provide improved preparation, detection, and response to cybersecurity threats; protecting its data, networks, and end users through governing access and implementing enhanced protections; and modernizing its core systems. Notably, the Judiciary Integrated Financial Management System (JIFMS) upgrade was completed in 2025; rollout of PACTS360, the probation and pretrial services case management system, began in February FY 2026 and is anticipated for completion in FY 2027; and the judiciary has made substantial progress on implementing a zero trust architecture to improve cybersecurity both inside and outside its network after completion of the National Active Directory Migration project in 2025.

The judiciary has been integrating one-time, non-recurring requirements into its annual budget request via a multiyear cybersecurity and IT modernization plan, last submitted in July 2025, totaling $516.0 million for FYs 2022-2027, of which $487.9 million is for the courts from the S&E account and $28.1 million is for the Defender Services account. At FY 2026 appropriations levels, the $28.1 million of Defender Services requirements are fully funded. Within the S&E account, $437.4 million[1] of the $487.9 million for the courts, will be funded through FY 2026, including $21.1 million in FY 2022, $106.1 million in FY 2023, $144.6 million[2] in FY 2024, $94.2 million in FY 2025, and $71.4 million in FY 2026.[3]

The FY 2027 request associated with the multiyear plan is $49.7 million, all within the S&E account. In FY 2026, several initiatives previously included in the multiyear plan are expected to be fully implemented and transitioned to recurring operations and maintenance that is budgeted for in the Infrastructure, Telecommunications, and Judicial Statistics and Reporting program components. The FY 2027 request includes funding for the following requirements:

- the judiciary's enhanced efforts to proactively identify and respond to identify external and internal threats;
- the Identity, Credential, and Access Management services across the judiciary that implement single sign-on, multi-factor authentication, and centralized user management with the goal of providing more secure authentication while reducing fraudulent activity;
- continued implementation of IT standardization that will improve the security of IT networks and systems; and

[1] Number excludes $0.3 million in FY 2024 technical adjustments.
[2] Number excludes $0.3 million in FY 2024 technical adjustments.
[3] The FY 2026 funded amount is slightly below the $72.3M included in the plan for that fiscal year. This is a result of lower than expected costs in one category of the plan, a change that will be reflected in the final version of the plan to be submitted following the FY 2027 budget request. This decrease in costs will also result in a decrease in the overall 5-year planned amount.

- continuing the modernization of core systems, which includes systems such as the Probation and Pretrial Services Automated Case Tracking System (PACTS), the debt collection system, the Jury Management System, and the Online System for Clerkship Application and Review (OSCAR).

An updated version of the multiyear plan will be submitted to Congress following submission of the FY 2027 budget request.

PACTS 360

For the last several years, the judiciary has provided updates on the efforts to stabilize and replace PACTS and ancillary applications. PACTS is the case management system used by approximately 8,000 probation and pretrial services officers and staff to conduct and manage investigations, risk assessments, and supervision of defendants and supervision of individuals on pretrial or post-conviction release. Currently more than 30 applications work together with PACTS to enable probation and pretrial services offices to perform their official duties. These applications, along with PACTS, have experienced recurring outages, slowdowns, and increasing costs to maintain the outdated systems. The judiciary has undertaken a two-phased approach to address problems with the reliability and performance of PACTS and the related applications. The first phase involved the stabilization of PACTS and existing applications. This has been completed, and the judiciary is now monitoring and maintaining the stable PACTS and existing applications. The second phase, which is ongoing, is to develop a replacement system for PACTS and the ancillary systems.

The judiciary continues to develop the various components of the cloud-based application (PACTS 360) chosen as the replacement system for PACTS. These components include the architecture, infrastructure, cybersecurity, data migration preparation, required business capabilities, implementation preparation, and training materials. The PACTS360 pilot went live in February 2026. The FY 2026 financial plan includes $28.6 million for:

1) continued product development, which includes the business, infrastructure, security capabilities, data migration, and development of user training material;
2) implementation of testing, monitoring, and cybersecurity; and
3) software subscriptions and cloud hosting services consumption for development and pre pilot activities.

The FY 2027 budget request includes $32.5 million in planned obligations for continuing district implementation; operations and maintenance for early phases of district implementation; Tier 2 help desk and operational monitoring support; and user training. PACTS 360 implementation is scheduled to be completed by the end of FY 2027.

Cybersecurity

The judiciary has been accelerating modernization efforts, placing heavy emphasis on incorporating cybersecurity in design, development, and execution. Due to concentrated cyber-attacks impacting judiciary systems and services, significant resources are still needed to ensure secure and resilient IT systems that support the judiciary's mission. Judiciary cyber-defenses continue to detect, deny, and withstand billions of attempted probes and attacks annually, and efforts have expanded to prevent further attempts by sharing knowledge about adversary tactics, techniques, and procedures with partner government agencies and the public. The volume of attacks against the judiciary remains steady, including sophisticated and complex attacks against the judiciary's public systems and services and its third-party cyber supply chain.

Cybersecurity activities and the employment of security-related assets are integral to the many IT systems, networks, and operations of the judiciary. The Judicial Conference has been progressively maturing the cybersecurity policies and IT technical standards that shape the overall security posture of the branch. As an enterprise, the judiciary continues to pursue modernization initiatives to adopt zero trust architecture, enhance visibility of all IT assets and services, upgrade endpoint protection capabilities into a unified integrated solution, and implement an enterprise-wide continuous diagnostics and mitigations program.

For FY 2027, the judiciary requests $121.8 million in appropriated S&E funding for cybersecurity (including $9.4 million of relevant activities from the Cybersecurity and IT Modernization multiyear plan), which is a net increase of $8.1 million above the FY 2026 financial plan level of $113.7 million. This request represents the subset of judiciary IT activities that meet a specified definition of cybersecurity, but many additional investments outside of these specific activities also help to improve the branch's cybersecurity posture. For example, the replacement of an outdated IT system with a more modern alternative may be done for operational reasons, but the new system may also offer better cybersecurity protections than the old version. In addition, further S&E cybersecurity activities may be funded with non-appropriated resources (primarily EPA fee collections) not included in the $121.8 million request. Additional cybersecurity funds are included in the budget accounts for CAFC, CIT, USSC, FJC, AO, Defender Services, and Court Security. As a result, the cybersecurity funding numbers presented here should not be read as a comprehensive total of every investment that contributes to judiciary cybersecurity, but rather as the total of investments targeted solely at cybersecurity and funded with appropriated S&E dollars.

The judiciary's cybersecurity efforts include:

- providing robust judiciary workforce training programs on cyber threats and best practices;
- issuing standard security toolsets;
- implementing next generation security architectures, such as zero trust architecture;
- monitoring judiciary devices 24 hours a day, seven days a week;
- promoting best practices and raising awareness of available patches and emerging threats;
- implementing multi-factor authentication across the judiciary;
- scanning programs and applications for vulnerabilities; and
- engaging independent third parties to perform periodic assessments.

Cybersecurity costs are separately presented in table 11.4, shown below, providing information detailing the judiciary's financial commitment to cybersecurity.[4] The $121.8 million of planned cybersecurity spending across S&E JITF program components accounts for 15.0 percent of the $810.7 million of total FY 2027 S&E JITF requirements. Cybersecurity resources are interspersed throughout the various IT program components and are a subset of the total requirements included in the program components shown in table 11.5 on page 11.16.

Table 11.4 S&E JITF Cybersecurity Requirements ($000)

IT Program Component ($000)	FY 2026 Plan	FY 2027 Request	Increase/Decrease
Judicial Statistics & Reporting Systems	316	320	4
Administrative & Management Systems	1,013	966	(47)
Telecommunications Program	53,870	55,843	1,973
Infrastructure & Collaboration Tools	47,953	53,373	5,420
Court Administration & Case Management	1,552	1,921	369
Cybersecurity & IT Modernization Plan	8,964	9,352	388
TOTAL, S&E JITF Cybersecurity	**113,668**	**121,775**	**8,107**

[4] Additional cybersecurity funds are included in the budget accounts for CAFC, CIT, USSC, FJC, AO, Defender Services, and Court Security as well as in the EPA Appendix. These amounts are not included in Table 11.4.

The FY 2027 S&E JITF cybersecurity request includes the following increases from the FY 2026 plan:

- $0.7 million net inflationary increase in Judicial Statistics and Reporting, Administrative and Management, Court Administration and Case Management systems, and Cybersecurity & IT Modernization Plan;
- $2.0 million net increase in the Telecommunications program associated with cyclical replacement of judiciary firewall service equipment; and
- $5.4 million net increase in the Infrastructure and Collaboration Tools program component associated with systems security testing, security assessments, and endpoint security services.

In addition to appropriated funding, in FY 2027, the judiciary plans to use $27.0 million of EPA fee collections for cybersecurity activities associated with security assets and operations to protect the Case Management/Electronic Case Files (CM/ECF) system and the Public Access to Court Electronic Records network, resulting in a total FY 2027 court cybersecurity program of approximately $148.8 million.

Chief Information Officer (CIO) Structural Realignment

Following a 2022 Government Accountability Office report, the judiciary established a Chief Information Officer (CIO). Appointment of a CIO was a significant step towards improving IT management and establishing enterprise oversight over the IT portfolio. Since that time, the AO evaluated and studied the AO's existing IT management and organizational structure as well as other CIO models. Ultimately, the AO determined that a realignment of the judiciary's IT structure and workforce was necessary. The existing structure presented challenges, and an improved CIO organizational structure will provide a better foundation for the judiciary's success. To support this effort, the judiciary developed and began implementation of a new IT organizational structure that ensures judiciary IT development and security functions report to the CIO. The objectives are better strategic planning, more efficient resource allocation, and improved coordination of technology initiatives that support the Judiciary's mission-critical objectives. The new structure aligns with business needs, separates service and product strategy from operations, and improves IT support services. This structure consolidates similar services and will enables the judiciary to be more responsive to changes in business demand or market conditions. Execution is underway, and the structural realignment is projected to be completed in FY 2026.

Case Management Modernization

The judiciary's electronic case management system dates back to the late 1980s. In September 1988, the Judicial Conference approved a new way of opening information to the public through a service known as PACER—Public Access to Court Electronic Records. To help manage caseloads the first tests of a computer-based case management system, which evolved into the current CM/ECF system, began in the mid-to-late 1990s. CM/ECF started rolling out to courts in 2001. In 2014, the judiciary began implementation of its first effort to update and improve CM/ECF through the Next Generation (NextGen) CM/ECF project.

In June 2019, the judiciary requested an independent assessment of CM/ECF. Among the analyses were three comprehensive reports by a technology consultancy within the General Services Administration. That reassessment process led to the current Case Management Modernization (CMM) effort to modernize case management and public access to case documents by replacing CM/ECF and PACER with new systems built on modern architecture. In late 2022, the judiciary communicated its vision to Congress and the courts for a cloud-based CMM system built using best practices such as user-centered design and iterative, agile development, and implemented using modern data standards with a data catalog and data governance framework. Since then, the judiciary has been making the necessary preparations for system development.

Recently, the judiciary has been the frequent target of highly sophisticated hackers who appear primarily to be seeking unauthorized access to "sealed" documents within CM/ECF. These cyber threats confirm that the existing CM/ECF and PACER systems are outdated and require replacement. Intensive efforts to modernize these systems are underway. Although the ultimate solution to the cybersecurity issues will be replacing CM/ECF with the CMM system, the judiciary is simultaneously securing CM/ECF as much as possible while building its successor.

The judiciary's current strategy is for new case management and PACER systems to be developed and rolled out on an incremental basis, meaning functionality of a modernized system is implemented in waves rather than the past model of deployment only after a system is fully designed, developed, and tested. This "agile" software development and implementation approach is consistent with current industry best practices. In addition, proper security controls within the new system are integrated as a critical part of the CMM system at every stage of development. The first incremental delivery of modules for the modernized case management system to pilot courts was in January 2026. Delivery to additional courts will occur in the coming fiscal years.

Based on the applicable court ruling[5] as well as the CMM requirements, the entire cost of the modernized system cannot be funded solely via PACER fee revenue. Expenses for elements of CMM that would be developed exclusively for internal judiciary use, i.e., expenses that have no nexus to the public's ability to access information on the federal courts' docketing system, cannot be funded with PACER fee revenue. Based on an initial judiciary review, some CMM requirements have an insufficient nexus to public access and require appropriated funding. For FY 2027, the judiciary is requesting $10.0 million to cover these CMM requirements.

Cloud Initiative

The judiciary has been operating a private cloud environment for many years, with physical locations in the two judiciary data centers. While the private cloud has adequately served the needs of the judiciary, access to public cloud services is necessary to take advantage of newer technologies which are not available in traditional on-premise data centers and to reduce dependence on the two data centers. The judiciary has developed a strategy to adopt public cloud services. The strategy focuses on a hybrid multi-cloud model that securely integrates the current on-premises judiciary private cloud with readily available modern and secure public cloud offerings. This integration will spur innovation, improve disaster recovery capabilities, and support a more mobile workforce, while ensuring maximum resilience and cost optimization.

The judiciary has awarded four open-market, multiple-award cloud blanket purchase agreements to procure services from the four major cloud service providers (CSPs). Since those contracts were awarded, the judiciary has implemented a centralized cloud service catalog with each CSP, which would enable judiciary units to select cloud services efficiently while eliminating the need for a prolonged requirement development period in new procurements and reducing contract administration on existing orders. This catalog is essential for scaling cloud adoption efficiently and maintaining judiciary-wide cost control and consistency. The catalogs are intended to be living documents that can be updated with new requirements and services over time. The catalog addresses these issues by creating a menu of services that can be quickly utilized and configured, as needed, by judiciary users on their cloud orders. In addition, the judiciary is engaging a Cloud Transformation/Build Integrator partner with expertise in cloud strategy execution, architecture design, migration, and integration services across hybrid and multi-cloud environments. This partnership is a key component of the judiciary's effort to modernize IT operations and is critical to de-risk the build-out phase and accelerate time-to-value. The goals of this transformation include strengthening cybersecurity, enhancing operational efficiency, and aligning more closely with the judiciary's mission in an increasingly dynamic digital landscape. The result of this partnership will allow the judiciary to rapidly leverage modern cloud

[5] *National Veterans Legal Services Program v. United States*, 291 F. Supp. 3d 123 (D.D.C. 2018), *aff'd and remanded,* 968 F.3d 1340 (Fed. Cir. 2020).

technologies to meet its evolving mission. The Cloud Transformation/Build Integrator's primary focus includes implementing secure network integration, identity integration and defining the optimal migration strategy for applications. The FY 2027 budget request includes $18.8 million to continue work on this ongoing initiative. This funding is essential to moving the project from the conceptual/design phase to full operational readiness. Critical investments in connectivity, associated hardware, infrastructure, and engineers will support:

- secure and resilient connectivity for integrated operations established through procurement of switches, routers and dedicated data circuits required to establish point-to-point, Secure Internet Protocol tunnels securely connecting the Internet Data Centers to the CSPs;
- cloud infrastructure and platform buildout to establish the core operating environments;
- cloud subject matter experts and transformation labor required to continue the complex public cloud build-out, including infrastructure-as-code deployments, security hardening and identity integration; and initial public cloud consumption costs for hosting foundational services and pilot workloads during the initial operational period.

JITF Program Requirements

The FY 2027 request reflects an essential growth in requirements for the ongoing demands of maintaining intricate data communications networks, operating systems, and effective and secure applications. To enable the courts to function most effectively, the judiciary has also taken an aggressive approach to maintaining and upgrading critical court support systems that provide financial reporting, personnel and payroll management, statistical reporting, and case management. A total of $705.8 million of base IT requirements are funded in FY 2026. This represents the amount that will be deposited in the JITF from the S&E account. The requirements for FY 2027 are $810.7 million. As shown in table 11.5, funding for the S&E JITF obligations supports eight program components described in more detail below.

Table 11.5 Salaries and Expenses Obligations – Information Technology Committee Requirements[6] ($000)

IT Program Component	FY 2026 Projected Obligations (Col A)	FY 2025 Slipped Requirements (Col B)	FY 2026 Base Requirements (Col A - Col B)	Change: FY 2026 Adj. Base Requirements to FY 2027 Current Services Requirements	FY 2027 Program Increases	FY 2027 Total Requirements
Judicial Statistics and Reporting Systems	15,984	228	15,756	4,987	-	20,743
Administrative and Management Systems	78,331	2,845	75,486	11,592	13,497	100,575
Telecommunications Program	117,221	1,790	115,431	6,876	-	122,307
Infrastructure and Collaboration Tools	185,242	3,726	181,516	18,098	19,204	218,818
Court IT Allotments	116,840	-	116,840	18,499	-	135,339
Court Administration and Case Management	22,917	-	22,917	24,736	-	47,653
Cybersecurity and IT Modernization Plan	104,580	33,165	71,415	(21,737)	-	49,678
Court Support Reimbursable Program	106,483	-	106,483	9,128	-	115,611
TOTAL, S&E JITF	**747,597**	**41,754**	**705,843**	**72,180**	**32,701**	**810,724**

The FY 2027 budget request is based on planned FY 2026 obligations. The FY 2026 funding level of $705.8 million will be deposited into the JITF from the S&E account.

[6] The associated pay and benefits and general inflation adjustments are combined with these increase requests. In line item 10 of the Salaries and Expenses chapter, pay and benefits and general inflation are not included in the IT requirements increases. Therefore, the numbers presented will not match.

FY 2027 S&E FUNDING REQUIREMENTS

The following sections present FY 2027 requirements for the S&E portion of the JITF. In total, requirements increase from a base level of $705.8 million in FY 2026 to $810.7 million in FY 2027. The FY 2027 request includes new program increases of $32.7 million associated with supporting the judiciary's Enterprise Learning Management System ($3.6 million), Judiciary Recruitment Management ($10.0 million), and IT Service Management (ServiceNow) platform ($8.1 million). The request also includes the re-request of program increases of $11.0 million associated with supporting the judiciary's integration into the public cloud. The following pages discuss significant changes between FY 2026 base requirements and FY 2027 requirements.

Judicial Statistical & Reporting Systems

FY 2027 Requirements: $20,743,000

Adjustments to Base from FY 2026: $4,987,000

Judicial statistical and reporting systems gather and report statistics in the judiciary; perform judiciary-wide data analyses and management reporting; and assist planning and decision-making with staffing, financial, and workload data.

The base increase of $4.7 million is associated with the EDW continuing to transition to the cloud and $0.3 million for inflationary costs.

Administrative & Management Systems

FY 2027 Requirements: $100,575,000

Adjustments to Base from FY 2026: $11,592,000

Program Increase: $13,497,000

Administrative and management systems include the judiciary's financial and personnel management systems, as well as systems to support and manage space and facilities projects, travel expenses, and judiciary websites.

The FY 2027 budget request includes adjustments to base to support the bi-annual version upgrade to the judiciary financial management system ($5.4 million); to support the clerkship application system ($3.1 million); for development services for SharePoint online ($1.5 million); and inflationary adjustments ($1.6 million).

The request also includes program increases totaling $13.5 million to support the development of the Judiciary Recruitment modernization initiative ($10.0 million) and the enterprise Learning Management System (LMS) ($3.5 million). The Judiciary Recruitment modernization initiative will assess personnel needs and develop a roadmap to provide the judiciary with centrally supported recruitment IT tools and services. Funds will be used to cover the costs of a centralized workforce data universe which will enable greater automation with workforce data, saving time and resources previously required to perform workforce analysis.

The procurement and configuration of an enterprise LMS will provide the judiciary with a unified platform to administer, document, track, and report training programs and content. It also offers classroom and online service capabilities. The enterprise LMS directly supports the implementation of recommendations of the Government Accountability Office and judiciary strategic planning and direction.

Telecommunications Program

FY 2027 Requirements: $122,307,000

Adjustments to Base from FY 2026: $6,876,000

The telecommunications program involves support for voice and data transmission services and telecommunications. The judiciary's communications program enables the judiciary to operate communications services for the appellate, district, and bankruptcy courts and for probation and pretrial services offices, as well as to procure communications equipment for new courthouses and courthouses undergoing major repairs and alteration. The increase in base requirements includes $4.5 million to fund security operations requirements and $2.4 to fund inflationary adjustments. This service will conduct full system lifecycle engineering and support functions to ensure that systems used can detect and counter adversary cybersecurity activity. They will also fulfill support requests for engineering and data analytic services through an Agile methodology. In addition, this service provides operations support for all managed security systems.

Infrastructure & Collaboration Tools

FY 2027 Requirements: $218,818,000

Adjustments to Base from FY 2026: $18,098,000

Program Increase: $19,204,000

New Program Increase: $8,233,000

Re-request: $10,971,000

Infrastructure and collaboration tools comprise the tools necessary to build and maintain a robust, reliable, and resilient judiciary-wide IT infrastructure. Included are the costs of hardware, software, and IT security associated with the judiciary's full enterprise hosting and cloud computing services and email and collaboration systems. This category also includes the costs of IT infrastructure for new courthouse construction projects and operating systems' support, maintenance, testing, and research.

In FY 2027, the base will increase due to the recategorization of requirements previously captured under the Cybersecurity and IT Modernization Priorities that are anticipated to be fully implemented in FY 2026. Components of the infrastructure base increase include recurring operations and maintenance ($7.3 million); ongoing implementation of enterprise project management ($3.8 million); continuation of web-based threat and endpoint protection services ($3.2 million); and inflationary adjustments ($3.8 million).

The request also includes program increases of $19.2 million in both new program increases and re-requested program increases. This includes funding to support the judiciary's integration into the commercial cloud ($11.0 million re-request); support the ServiceNow platform (new request $8.1 million); and support for the development of an enterprise learning management system (LMS) (new request $0.1 million).

As described on page 11.14, the judiciary's integration into a public cloud will integrate the current on-premises judiciary private cloud with readily available modern and secure public cloud offerings, which will spur innovation, improve continuity of court operations and disaster recovery capabilities, and support a more mobile workforce. Requested funds will support the procurement of hardware, infrastructure, and engineering support for the integration into a public cloud. (Re-request)

ServiceNow is a cloud-based workflow platform that consists of modules. Each module offers capabilities that can be deployed across the judiciary to fulfill various business needs. The judiciary has successfully deployed the ServiceNow module to the National Service Desk to coordinate service requests on national applications. The new platform will increase efficiency by: offering automation of processes and smart workflows resulting in shorter response and resolution time; utilizing a virtual agent where all users can request a service, find the status of an issue, and find knowledge articles; empowering users with a robust search engine to quickly find and access relevant knowledge articles; and enabling use of an app for incident or service request creation, tracking statuses, and approvals.

The enterprise LMS funding will comply with Government Accountability Office audit requirements for tracking training metrics, specifically in relation to cybersecurity training mandates. An LMS allows the judiciary training staff to assign courses, manage course registrations, track attendance in mandatory training courses, and issue certificates of completion.

Court IT Allotments

FY 2027 Requirements: $135,339,000

Adjustments to Base from FY 2026: $18,499,000

Court IT allotments cover costs paid directly by 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, maintenance, and courtroom technology.

The base adjustment includes recurring IT infrastructure and maintenance expenses ($14.0 million); maintenance, cyclical replacement, and upgrade of courtroom technologies ($2.0 million); and inflationary adjustments ($2.5 million).

Court Administration & Case Management

FY 2027 Requirements: $47,653,000

Adjustments to Base from FY 2026: $24,736,000

Court administration and case management contains a variety of tools, including PACTS 360, to access critical case information

and law enforcement databases; systems for juror qualification, management, and payment; tools for jury participants to communicate with the courts; as well as eVoucher, the system that captures requests for payments to private court-appointed counsel and expert service providers.

The base adjustment of $24.7 million includes funding reallocated from the Cybersecurity and IT Modernization Plan component for modernizing the judiciary's Case Management Modernization (CMM) initiative ($10.0 million); probation and pretrial applications not subsumed into the modernized PACTS 360 ($7.5 million); and supporting PACTS 360 integration and operations and maintenance activities ($4.8 million). Funds will also be used to support other components including eVoucher enhancements and security updates ($2.0 million); and inflationary adjustments ($0.4 million).

Cybersecurity & IT Modernization Plan

FY 2027 Requirements: $49,678,000

Adjustments to Base from FY 2026: ($21,737,000)

The cybersecurity and IT modernization plan is the judiciary's multiyear cybersecurity and IT modernization plan (referenced on page 11.7). As outlined in the plan, these funds will be dedicated to high-priority cybersecurity efforts and modernizing aging legacy systems or applications that are based on vulnerable programming technologies or technologies that are becoming obsolete.

The base in this category decreases by a net of $21.7 million due to requirements previously included in this component that are expected to be fully implemented in FY 2026 and will be tracked as recurring operations and maintenance in other program components beginning in FY 2027. The proposed decrease also reflects a reallocation of $10.0 million in CMM-related costs funded under this component in FY 2026 but that will now be tracked in the Court Administration & Case Management component for FY 2027 and future fiscal years.

Court Support Reimbursable Program

FY 2027 Requirements: $115,611,000

Adjustments to Base from FY 2026: $9,128,000

This category funds AO staff that provide IT development, management, and maintenance services to the courts. These services include IT policy and planning guidance; architecture and infrastructure support; security services; development, testing, and implementation of national IT applications; IT training; and other administrative and IT support services on behalf of the courts.

The FY 2027 budget request for the court support reimbursable program includes $115.6 million for the salaries, benefits, and related expenses of AO staff that are reimbursed from the S&E account. The $9.1 million increase in FY 2027 is due to $7.9 million to restore base requirements and $1.2 million for standard pay and benefit increases for existing reimbursable positions.

PROGRAMS FUNDED FROM DEPOSITS FROM OTHER JUDICIARY ACCOUNTS

Organizations within the judiciary that are not mandatory users of the JITF may deposit funds to assist them in managing their IT efforts. In recent years, the following organizations and programs have made such deposits.

Administrative Office of the U.S. Courts

At the beginning of FY 2026, the AO had $3.9 million available in JITF carryforward balances. In FY 2026, the AO intends to obligate the entire amount to refresh AO computers, laptops, printers, and related equipment pursuant to an approximate four-year replacement cycle, as well as copiers, video conferencing equipment, and software as required. The AO currently does not anticipate an end-of-year balance to be carried forward into FY 2027.

CAFC

CAFC anticipates obligating $2.6 million from the JITF in FY 2027. The CAFC has, and will continue to pursue, the most effective cybersecurity protocols, architecture, and software.

Obligations under JITF will be dedicated to deploying advanced endpoint protection and response software, upgrading wireless and VoIP infrastructure, replacing the CAFC's existing multi-function printers with models fully integrated with Microsoft Azure cloud services, covering ongoing IT equipment maintenance expenses, and upgrading critical hardware components.

An increased portion of JITF resources will be used to implement an upgrade to the court's case management and filing system, including development costs, security validation, ongoing maintenance expenses, and IT training to maintain and enhance staff capabilities in emerging development and security technologies.

CIT

At the beginning of FY 2026, $1.1 million was available in JITF carryforward balances. Of this amount, CIT is planning to obligate $1.0 million from the JITF in FY 2026 to:

- install audio/video technology for use in courtrooms;
- purchase licenses to maintain the court's IT hardware and software applications;
- maintain and support digital recording systems, data network and voice connections, VPN System, VOIP telephone system, and Judiciary DCN; and
- procure computer desktop systems and laptops according to the judiciary's cyclical replacement program.

At the beginning of FY 2027, the CIT anticipates that $131,000 will be available in carryforward balances in the JITF. These funds will be used to continue CIT's IT initiatives as described above and to support its short-term and long-term IT needs.

FJC

At the beginning of FY 2026, the FJC had $949,000 available in carryforward balances from the JITF. The FJC plans to obligate $626,000 in FY 2026. The FJC has no plans to utilize JITF funds FY 2027.

USSC

At the beginning of FY 2026, USSC had $1.7 million available in carryforward balances from the JITF. The Commission plans to use the entire $1.7 million during FY 2026 to continue and renew information technology, cybersecurity, and data collection projects that cannot be covered by the annual appropriation due to funding constraints.

Key cybersecurity initiatives include strengthening security processes and protocols, leveraging recent developments in encryption technology, and auditing authorized users to prevent data compromises. In addition, the Commission is continuing the parallel data extraction project that began in FY 2024. Furthermore, in FY 2026, the Commission is undertaking the following technology projects: data warehousing; database enhancements and maintenance; uninterruptible power supply upgrades; other efforts to enhance the security of the Commission's internal systems; and a complete redesign and replacement of the video presentation, video conferencing, and audio-conferencing systems in the Commission's main conference room.