

## **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 information technology resources. The JITF makes it possible to manage the IT program over a multiyear 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 (EPA) 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 2024 through the FY 2026 request. Tables 11.2 and 11.3 provide additional data about obligations and outlays.

**Table 11.1 Judiciary Information Technology Fund  
Obligations and Financing (\$000)**

<b>Description</b>	<b>FY 2024 Actual</b>	<b>FY 2025 Plan</b>	<b>FY 2026 Request</b>
<b><u>Obligations:</u></b>			
Salaries & Expenses Requirements (with carryforward)	711,339	734,191	777,976
Electronic Public Access (EPA) Program	161,651	238,830	231,003
Administrative Office of the U.S. Courts	6,033	2,872	-
Court of Appeals for the Federal Circuit	2,622	2,290	1,153
Court of International Trade	1,458	1,418	130
Federal Judicial Center	38	-	-
U.S. Sentencing Commission	200	1,844	-
<b>TOTAL JITF</b>	<b>883,342</b>	<b>981,445</b>	<b>1,010,262</b>
<b><u>Financing:</u></b>			
<i>Salaries and Expenses</i>			
Unobligated Balance, Start of Year	157,604	152,164	20,000
New Deposits and Prior Year Recoveries	705,898	602,027	757,976
Unobligated Balance, End of Year	(152,164)	(20,000)	-
<b>Total Salaries &amp; Expenses</b>	<b>711,339</b>	<b>734,191</b>	<b>777,976</b>
<i>EPA Program</i>			
Unobligated Balance, Start of Year	149,434	161,987	80,157
Estimated Receipts and Prior Year Recoveries	174,204	157,000	166,000
Unobligated Balance, End of Year	(161,987)	(80,157)	(15,154)
<b>Total EPA Program</b>	<b>161,651</b>	<b>238,830</b>	<b>231,003</b>
<i>Administrative Office of the U.S. Courts</i>			
Unobligated Balance, Start of Year	6,552	2,872	-
New Deposits and Prior Year Recoveries	2,353	-	-
Unobligated Balance, End of Year	(2,872)	-	-
<b>Total Administrative Office of the U.S. Courts</b>	<b>6,033</b>	<b>2,872</b>	<b>-</b>

<i>Court of Appeals for the Federal Circuit</i>			
Unobligated Balance, Start of Year	4,350	3,443	1,153
New Deposits and Prior Year Recoveries	1,715	-	-
Unobligated Balance, End of Year	(3,443)	(1,153)	-
<b>Total Court of Appeals for the Federal Circuit (Non- EPA)</b>	<b>2,622</b>	<b>2,290</b>	<b>1,153</b>
<i>Court of International Trade</i>			
Unobligated Balance, Start of Year	1,765	1,488	100
New Deposits and Prior Year Recoveries	1,180	30	30
Unobligated Balance, End of Year	(1,488)	(100)	-
<b>Total Court of International Trade (Non- EPA)</b>	<b>1,458</b>	<b>1,418</b>	<b>130</b>
<i>Federal Judicial Center</i>			
Unobligated Balance, Start of Year	987	949	949
New Deposits and Prior Year Recoveries	-	-	-
Unobligated Balance, End of Year	(949)	(949)	(949)
<b>Total Federal Judicial Center</b>	<b>38</b>	<b>-</b>	<b>-</b>
<i>U.S. Sentencing Commission</i>			
Unobligated Balance, Start of Year	1,669	1,844	-
New Deposits and Prior Year Recoveries	375	-	-
Unobligated Balance, End of Year	(1,844)	-	-
<b>Total U.S. Sentencing Commission</b>	<b>200</b>	<b>1,844</b>	<b>-</b>
<b>GRAND TOTAL JITF</b>	<b>883,342</b>	<b>981,445</b>	<b>1,010,262</b>

### Obligations by Budget Object Class (\$000)

Description	FY 2024 Actual	FY 2025 Plan	FY 2026 Request
21.0 Travel and Transportation of Persons	4,915	5,461	5,621
23.3 Communications, Utilities, and Misc. Charges	61,685	68,536	70,548
24.0 Printing and Reproduction	5,309	5,899	6,072
25.1 Advisory and Assistance Services	454,315	504,771	519,592
25.3 Other Goods and Services from Federal Sources	111,181	123,529	127,156
25.7 Operation and Maintenance of Equipment	6,751	7,501	7,721
26.0 Supplies and Materials	7,274	8,082	8,319
31.0 Equipment	231,912	257,668	265,234
<b>Total Obligations</b>	<b>883,342</b>	<b>981,445</b>	<b>1,010,262</b>

**Table 11.3 Judiciary Information Technology Fund  
Relation of Obligations to Outlays (\$000)**

	<b>FY 2024 Actual</b>	<b>FY 2025 Plan</b>	<b>FY 2026 Request</b>
Direct Obligations Incurred	883,342	981,445	1,010,262
Obligated Balance, Start of Year	452,722	541,612	699,253
Adjustments of Prior Year Activity	(61,567)	-	-
Obligated Balance, End of Year	(541,612)	(699,253)	(835,613)
<b>Total Outlays</b>	<b>732,885</b>	<b>823,804</b>	<b>873,902</b>
Less Offsets	(23,861)	-	-
Net Outlays	709,024	823,804	873,902

## **PROGRAMS FUNDED FROM THE SALARIES AND EXPENSES 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.

The judiciary continues to develop critical improvements to court support systems; including the financial management system, probation and pretrial services case management system, and court case management systems; as well as support essential cybersecurity programs.

## 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 progress on the requirements outlined within the Strategy. Two initiatives that have been completed are the Data Center Move and the establishment of the Enterprise Communications and Coordination Center. Notable projects underway include modernizing legacy court and administrative systems, such as the judiciary's financial management system, the fingerprint

management system, and judiciary workforce planning; improving and creating segmented network security for specific systems; and providing security tools to protect all devices and systems connecting to the judiciary's network.

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 2024, totaling \$470.2 million for FYs 2022-2027, of which \$442.1 million is for the courts from the S&E account and \$28.1 million is for the Defender Services account. Of the \$442.1 million for the courts, \$366.0 million<sup>1</sup> is assumed to have been funded to date, including \$21.1 million in FY 2022, \$106.1 million in FY 2023, \$144.6 million<sup>2</sup> in FY 2024, and \$94.2 million<sup>3</sup> in FY 2025.

Beginning in FY 2026, several initiatives previously included in the multiyear plan are expected to be fully implemented and will transition to recurring operations and maintenance that is budgeted for in the Infrastructure, Telecommunications, and Judicial Statistics and Reporting program components. Requirements that have transitioned to operations and maintenance include:

- Expansion of the EDW;
- Implementation of a cloud-based backup solution;
- Judiciary standard IT security services and improved password management;
- National messaging and collaboration system upgrade;
- Red Team IT security protection;
- Acceleration of court unit assessments; and
- Information protection and governance services; security data analytics; and security operations center engineering support.

The FY 2026 request associated with the multiyear plan is \$72.3 million, which is \$30.1 million higher than the FY 2026 requirements identified in the July 2024 submission (\$72.3 million versus the estimated \$42.2 million). The projected costs for implementing the Strategy have increased in FY 2026 due to the inclusion of requirements related to supporting initiatives currently underway in FY 2025. Several factors have increased costs including changes in scope, higher inflation rates, and rising costs of technology. An updated version of the multiyear plan will be submitted to Congress following the enactment of the final FY 2025 appropriations.

---

<sup>1</sup> Number excludes \$0.3 million in FY 2024 technical adjustments.

<sup>2</sup> Number excludes \$0.3 million in FY 2024 technical adjustments.

<sup>3</sup> Number excludes \$0.3 million in FY 2024 technical adjustments.

### ***PACTS 360***

For the last several years, the judiciary has provided updates on the efforts to stabilize and replace the Probation and Pretrial Services Automated Case Tracking System (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 there are more than 30 applications that 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 ancillary applications. The first phase involves 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 FY 2025 assumed obligations include \$31.2 million for:

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

The FY 2026 budget request includes \$27.0 million with planned obligations for pilot and districts 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.

### ***Judiciary Integrated Financial Management System Upgrade***

The judiciary is implementing a technical upgrade to the Judiciary Integrated Financial Management System (JIFMS), the judiciary's official budget, accounting, and procurement system. The upgrade of JIFMS from version 7.0.2 (released in September 2010) to version 8.1.4 is critical to address numerous audit/security concerns, technical obsolescence of third-party support tools, performance concerns, and government compliance functionality. The age of the system and the supporting third-party tools inhibit compliance with judiciary security standards, exposing the judiciary to potential cyber risks.

Existing audit and IT security findings will be remediated with the upgrade of the system, improving both operational and technical efficiencies while strengthening the judiciary's cyber security posture. With this upgrade, the judiciary will comply with the government wide G-Invoicing (a web-based application for federal agencies to buy or sell from each other) mandate to support agency-to-agency Intergovernmental Payment and Collections transactions. A major upgrade is a foundational step to incorporate future incremental upgrades at a more manageable and predictable cost as part of the operations and maintenance cycle.

The upgrade is scheduled to be fully implemented across the judiciary by July 2025. The project is currently on schedule and within budget. The judiciary's FY 2026 budget request includes \$7.3 million to fund post-implementation development activities to enable the introduction of enhancements.

### ***Data Center Move***

The judiciary has two internet data centers, which are geographically dispersed to serve the eastern and western halves of the country. In 2018, AT&T, the owner of the judiciary data center in San Diego, California, sold the facility and notified the judiciary that it must move out by July 2024. In June 2022, the judiciary was notified that the move out date was changed to December 2023, creating a much tighter timeline. The judiciary was required to migrate the San Diego data center to a new location in El Segundo, California, which was relatively close to the current data center and facilitated a move that minimized disruption to the courts.

In July 2023, the judiciary began shutting down equipment/systems in the San Diego data center. In August 2023, all services in San Diego were shut down and all judiciary services were operating out of the Ashburn data center. The judiciary started the equipment move to El Segundo, and the move was completed in September 2023. All court and national applications and services were successfully moved back to the new west coast data center in August 2024.

The judiciary required substantial resources to complete the data center move, including funding for additional hardware to stand up a new data center, contractual labor to support the move, and federal staff to coordinate the effort. The move was completed on schedule and within budget.

### *Cybersecurity*

The judiciary has been modernizing its cybersecurity operations and is continually strengthening its cybersecurity posture. Sustaining these efforts and implementing additional security-related initiatives continues to require significant resources. Like other commercial and government entities, the judiciary is targeted repeatedly by attempted cyberattacks against its information systems, judges, and other personnel. Judiciary cyber-defenses blocked approximately 200 million harmful events from reaching court local area networks in FY 2024. This number was nearly identical to the numbers reported in the previous year. Though the numbers targeting the judiciary remained steady, the sophistication of the attacks and attacks against the judiciary's supply chain and third-party partners has increased as hackers sought new ways to disrupt U.S. government functionality and judiciary operations.

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 requires all judiciary organizations to conduct annual security awareness training and maintain the security health of their local area networks. As an enterprise, the judiciary is actively pursuing modernization initiatives to adopt zero trust architecture principles while at the local court level, court units receive enterprise-license security software for endpoint protection, web-based threat protection, patch and asset management and vulnerability scanning.

For FY 2026, the judiciary requests \$119.4 million in appropriated S&E funding for cybersecurity (including \$18.1 million of relevant activities from the Cybersecurity and IT Modernization multiyear plan), which is a net increase of \$ 0.5 million above the FY 2025 financial plan level of \$118.9 million. This request represents the subset of judiciary IT activities that meet a specified definition of cybersecurity, but 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 \$119.4 million request. 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<sup>4</sup>. Within the courts' S&E account, cybersecurity accounts for 15.3 percent of the total FY 2026 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 11.15.

**Table 11.4 Salaries and Expenses JITF Cybersecurity Requirements (\$000)**

<b>IT Program Component (\$000)</b>	<b>FY 2025 Plan</b>	<b>FY 2026 Request</b>	<b>Increase/Decrease</b>
Judicial Statistics & Reporting Systems	317	319	2
Administrative & Management Systems	782	1,089	307
Telecommunications Program	63,905	50,435	(13,470)
Infrastructure & Collaboration Tools	27,363	47,684	20,321
Court Administration & Case Management	1,572	1,715	143
Cybersecurity & IT Modernization Plan	24,963	18,149	(6,814)
<b>TOTAL, S&amp;E JITF Cybersecurity</b>	<b>118,902</b>	<b>119,391</b>	<b>489</b>

The FY 2026 S&E JITF cybersecurity request includes adjustments as follows:

---

<sup>4</sup> Additional cybersecurity funds are included, but not displayed separately, in the budget accounts for CACF, CIT, USSC, FJC, AO, Defender Services, and Court Security as well as in the EPA Appendix.

- \$0.5 million net inflationary increase in Judicial Statistics and Reporting, Administrative and Management, Court Administration and Case Management systems;
- \$13.5 million net decrease in the Telecommunications program associated with non-recurring cybersecurity costs expected to be obligated in FY 2025;
- \$20.3 million net increase in the Infrastructure and Collaboration Tools program component is associated with the shift of cybersecurity related requirements previously included in the Cybersecurity and IT Modernization Priorities component that are expected to complete implementation in FY 2025 and will become recurring operations and maintenance; and
- \$6.8 million net decrease in Cybersecurity & IT Modernization Plan due to cybersecurity related requirements previously included in this component that are expected to complete implementation in FY 2025 and will become recurring operations and maintenance costs in other program components.

Additionally, in FY 2026, the judiciary plans to use \$29.5 million of EPA fee collections (compared to \$33.6 million in FY 2025) for cybersecurity activities associated with security assets and operations to protect the Case Management/Electronic Case Files system and the Public Access to Court Electronic Records network, resulting in a total FY 2026 court cybersecurity program of approximately \$148.9 million.

### ***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 judiciary's design and implementation of a hybrid multi- 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.

In 2023, the judiciary awarded four open-market, multiple-award cloud blanket purchase agreements (BPAs) to procure services from the four major cloud service providers (CSPs). Since those contracts were awarded, the judiciary has established testing environments to help establish the policies and procedures necessary to manage the technical infrastructure for each CSP. In addition, the testing environments will be used to determine how best to connect each CSP with the judiciary's internal infrastructure, such as the data communications network (DCN) and identity management systems. The judiciary is eager to begin using cloud services to support modernization projects. Four major projects that require the use of the commercial cloud include Case Management Modernization

(CMM), PACTS360, the modernized Enterprise Data Warehouse (EDW), and eVoucher. Efforts are underway to begin providing these projects with non-production cloud environments, where they can begin testing cloud services.

The judiciary is taking a methodical approach to establishing the cloud infrastructure and defining operational procedures to help avoid the pitfalls other government agencies have experienced. The challenges endured by other government agencies include issues in the areas of financial management for a consumption-based cost model, security, and acquisitions challenges to manage a dynamic portfolio of solutions provided by the cloud service providers. The judiciary is working closely with project teams to provide adequate cloud capabilities so that modernization efforts can continue, while also working to avoid potential operational and security challenges. Given these complexities, the judiciary is working to establish the foundation of these cloud environments by the end of FY 2025.

The FY 2026 budget request includes \$20.6 million for connectivity, associated hardware, infrastructure, and engineers to support:

- the cloud infrastructure;
- the procurement of routers and data circuits required to provide connectivity to CSP partners to create point-to-point Internet Protocol tunnels securely connecting the Internet Data Centers to CSPs;
- cloud subject matter experts (contractors) required to continue public cloud buildout; and
- contract costs associated with using a public cloud service provider.

### ***JITF Program Requirements***

The FY 2026 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 \$697.2 million of base IT requirements are funded in the enacted FY 2025 appropriations bill. This represents the amount that will be deposited in the JITF from the S&E account. The requirements for FY 2026 are \$778.0 million. As shown in table 11.5, funding for the S&E JITF obligations supports eight program components described in more detail below.

<b><u>IT Program Component</u></b>	<b>FY 2025 Projected Obligations (Col A)</b>	<b>FY 2024 Slipped Requirements (Col B)</b>	<b>FY 2025 Base Requirements (Col A - Col B)</b>	<b>Change: FY 2025 Adj. Base Requirements to FY 2026 Current Services Requirements</b>	<b>FY 2026 Program Increases</b>	<b>FY 2026 Total Requirements</b>
Judicial Statistics and Reporting Systems	13,305	-	13,305	4,222	-	17,527
Administrative and Management Systems	77,971	2,046	75,925	6,040	1,313	83,278
Telecommunications Program	134,231	2,802	131,429	(5,933)	-	125,496
Infrastructure and Collaboration Tools	147,139	14,148	132,991	53,565	20,033	206,589
Court IT Allotments	114,672	746	113,926	16,932	-	130,858
Court Administration and Case Management	24,507	2,664	21,843	4,590	-	26,433
Cybersecurity and IT Modernization Priorities	130,451	36,288	94,163	(21,866)	-	72,298
Court Support Reimbursable Program	113,596	-	113,596	1,899	-	115,495
<b>TOTAL, S&amp;E JITF</b>	<b>755,872</b>	<b>58,694</b>	<b>697,178</b>	<b>59,452</b>	<b>21,346</b>	<b>777,976</b>

The FY 2026 budget request is based on the enacted FY 2025 appropriations bill and the FY 2025 financial plan. The FY 2025 financial plan assumes \$697.2 million will be deposited into the JITF from the S&E account.

The following sections present FY 2026 requirements for the S&E portion of the JITF. In total, requirements increase from a base level of \$697.2 million in FY 2025 to \$778.0 million in FY 2026. The FY 2026 request includes program increases of \$21.3 million associated with supporting the judiciary’s integration into the public cloud (\$14.4 million), the creation of a Development, Security, and Operations (DevSecOps) framework (\$1.3 million), the IT Service Management platform (\$4.3 million), and development of a national budget formulation and execution system (\$1.3 million). The following pages discuss significant changes between the FY 2025 base requirements and the FY 2026 requirements.

### ***Judicial Statistical & Reporting Systems***

**FY 2026 Requirements:** **\$17,527,000**

**Adjustments to Base from FY 2025:** **\$4,222,000**

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 increased by \$4.2 million to include the recategorization of requirements previously captured under the Cybersecurity and IT Modernization Priorities that are anticipated to be fully implemented in FY 2025 for the modernized EDW operations and maintenance (\$2.1 million); integrate legacy PACTS and PACTS 360 data into the EDW for analytical research, trend reporting, statistical reporting, and other data dependent activities (\$1.2 million); and the EDW initial transition to the cloud (\$0.9 million).

### ***Administrative & Management Systems***

**FY 2026 Requirements:** **\$83,278,000**

**Adjustments to Base from FY 2025:** **\$6,040,000**

**Program Increase:** **\$1,313,000**

Administrative and management systems includes 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 2026 budget request includes \$2.9 million for JIFMS upgrade post implementation development, \$1.5 million for judiciary financial disclosure system operational support, and \$1.6 million for inflationary adjustments.

The request also includes a program increase of \$1.3 million to support the development and implementation of a national budget formulation and execution system with full integration to JIFMS and key budget execution processes, as well as inclusion of scenario analyses, program-specific reporting, and additional decision support capabilities.

### ***Telecommunications Program***

**FY 2026 Requirements:** **\$125,496,000**

**Adjustments to Base from FY 2025:** **(\$5,933,000)**

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 \$5.9 million decrease to the base is due to the anticipated completed transition from the Networx contract to the Enterprise Infrastructure Services contract.

### ***Infrastructure & Collaboration Tools***

**FY 2026 Requirements:** **\$206,589,000**

**Adjustments to Base from FY 2025:** **\$53,565,000**

**Program Increase:** **\$20,033,000**

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

In FY 2026, 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 2025. Components of the infrastructure base increase are recurring operations and maintenance (\$36.1 million); strengthening early detection, diagnosis, and response capabilities to manage application performance problems and cybersecurity events (\$5.6 million); rising contract costs (\$5.0 million); continuing development of the

framework needed to implement an enterprise wide enterprise architecture program (\$3.9 million); inflationary adjustments (\$2.8 million); and support for external cybersecurity testing and assessments (0.2 million).

The request also includes program increases of \$20.0 million to support the judiciary's integration into the public cloud (\$14.4 million), the creation of a DevSecOps framework (\$1.3 million), and the IT Service Management (National IT Tracking System) platform (\$4.3 million).

As described on page 11.13, 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.

DevSecOps is shorthand for "Development, Security, and Operations," a framework for approaching building or modifying any IT application. The framework requires the integration of security into all phases of any application's full development lifecycle. The previous way of approaching IT upgrades was to build an application's functionality and then find ways to secure it. The DevSecOps framework, by contrast, requires incorporating security features from the very beginning and maintaining them throughout the life of the application. The program increase will fund the continued support for the creation of a DevSecOps framework within the judiciary. The funding requested supports DevSecOps subject

matter experts, ongoing training and implementation, and licenses for continuous integration/continuous delivery (CI/CD) pipeline tools in support of the ongoing implementation. Requirements include contractors that will provide resources to support the ongoing engineering, architecture, governance, training, and implementation efforts.

The judiciary is implementing a national IT tracking system, which 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 IT Service Management module to the National Service Desk to coordinate service requests on national applications. The program increase for the national IT tracking system supports the implementation of two additional modules. The IT Operations Management module focuses on implementation and maintenance. This module automates the monitoring and lifecycle management for IT services, applications, and infrastructure, and helps ensure they are stable and available for use. The IT Assets Management module is focused on asset management and automates the process of accounting for assets during their lifecycle. This includes procurement and purchasing, software license management, technology refresh, and asset valuation. The implementation of the national IT tracking system modules vastly improves IT management across the judiciary.

#### ***Court IT Allotments***

**FY 2026 Requirements:** **\$130,858,000**

**Adjustments to Base from FY 2025:** **\$16,932,000**

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 (\$10.0 million), IT office supplies and maintenance (\$4.6 million), and inflationary adjustments (\$2.4 million).

#### ***Court Administration & Case Management***

**FY 2026 Requirements:** **\$26,433,000**

**Adjustments to Base from FY 2025:** **\$4,590,000**

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 \$4.6 million is associated with modernizing probation and pretrial services applications not subsumed into the modernized PACTS 360 (\$3.5 million) and rising contract costs (\$1.1 million).

#### ***Cybersecurity & IT Modernization Plan***

**FY 2026 Requirements:** **\$72,298,000**

**Adjustments to Base from FY 2025:** **(\$21,866,000)**

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 a net \$21.9 million due to requirements previously included in this component that are expected to be fully implemented in FY 2025 and will be tracked as recurring operations and maintenance in other program components beginning in FY 2026.

#### ***Court Support Reimbursable Program***

**FY 2026 Requirements:** **\$115,495,000**

**Adjustments to Base from FY 2025:** **\$1,899,000**

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 2026 budget request for the court support reimbursable program includes \$115.5 million for the salaries, benefits, and

related expenses of AO staff that are reimbursed from the Salaries and Expenses account. The \$1.9 million increase in FY 2026 is due to employee benefits changes and inflation.

#### **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.

##### ***Court of Appeals for the Federal Circuit***

CACF anticipates obligating \$1,153,000 from the JITF in FY 2026. This amount includes increased costs for the courtroom technology upgrade project and upgrades to IT cybersecurity, network and efforts related to the IT Scorecard.

Obligations will also include the annual renewal of software licenses such as Office 365 and many other software packages integral to court operations, and IT-related training and travel for all staff. Finally, IT equipment maintenance expenses will be paid using funds from the JITF.

##### ***Court of International Trade***

At the beginning of FY 2025, \$1,488,000 was available in JITF carryforward balances. CIT is planning to obligate \$1,418,000 from the JITF in FY 2025 to:

- install audio/video technology for use in courtrooms and conference rooms;

- purchase licenses to maintain the court’s IT hardware and software applications;
- replace network switches that have reached end of life;
- 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 2026, the Court anticipates that \$100,000 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.

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

At the beginning of FY 2025, the AO had \$2,872,000 available in JITF carryforward balances. In FY 2025, 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 2026.

#### ***Federal Judicial Center***

At the beginning of FY 2025, the FJC had \$949,000 available in carryforward balances from the JITF. The FJC has no plans to utilize JITF funds in FY 2025 or FY 2026.

#### ***U.S. Sentencing Commission***

At the beginning of FY 2025, \$1,844,000 was available in carryforward balances from the JITF. Of this amount, USSC is planning to use the entire \$1,844,000 during FY 2025 to support continued efforts in cybersecurity and other IT related projects.

Key cybersecurity initiatives include strengthening security processes and protocols, leveraging recent developments in encryption technology, and auditing authorized users to avoid data compromises. In addition, USSC is committed to completing a major parallel data extraction project started in FY 2024. Furthermore, USSC is undertaking the following technology projects in FY 2025: Data warehousing, database enhancements and maintenance, and other efforts to enhance the security of USSC’s internal systems; the replacement of outdated VOIP telephone system; and the potential redesign and replacement of the video presentation and video and audio-conferencing systems in USSC’s main conference room.