

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 authority of the JITF 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 fund makes it possible to manage the IT program over a multi-year planning cycle, which allows more effective and efficient planning, budgeting, and use of funds 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.

Requirements are financed via the JITF 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 information (see Appendix 2, Electronic Public Access for more information on this program);
- unobligated balances in the fund 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 program; and
- deposits from other judiciary appropriations that are non-mandatory judiciary users of the fund (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 on the following pages displays JITF requirements and funding sources for FY 2021 through the FY 2023 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)

	FY 2021 Actual	FY 2022 Assumed Obligations	FY 2023 Request
<u>Obligations:</u>			
Salaries & Expenses Requirements (with carryforward)	512,844	627,955	653,984
EPA Program	129,640	219,298	182,240
Administrative Office of the U.S. Courts	4,214	2,002	0
Court of Appeals for the Federal Circuit	964	0	689
Court of International Trade	613	915	167
Court Security	0	101	0
Federal Judicial Center	0	250	0
U.S. Sentencing Commission	0	1,669	0
TOTAL JITF	648,275	852,190	837,080
<u>Financing:</u>			
Salaries and Expenses			
Unobligated Balance, Start of Year	63,701	65,616	20,000
New Deposits and Prior Year Recoveries	514,759	582,339	633,984
Unobligated Balance, End of Year	-65,616	-20,000	0
Total Salaries & Expenses	512,844	627,955	653,984
EPA Program			
Unobligated Balance, Start of Year	136,512	152,482	77,684
Estimated Receipts and Prior Year Recoveries	145,610	144,500	144,500
Unobligated Balance, End of Year	-152,482	-77,684	-39,944
Total EPA Program	129,640	219,298	182,240
Administrative Office of the U.S. Courts			
Unobligated Balance, Start of Year	4,626	2,002	0
New Deposits and Prior Year Recoveries	1,590	0	0
Unobligated Balance, End of Year	-2,002	0	0
Total Administrative Office of the U.S. Courts	4,214	2,002	0

	FY 2021 Actual	FY 2022 Assumed Obligations	FY 2023 Request
Court of Appeals for the Federal Circuit			
Unobligated Balance, Start of Year	3,817	4,342	4,342
New Deposits and Prior Year Recoveries	1,489	0	0
Unobligated Balance, End of Year	-4,342	-4,342	-3,653
Total Court of Appeals for the Federal Circuit (non-EPA)	964	0	689
Court of International Trade			
Unobligated Balance, Start of Year	1,191	1,082	167
New Deposits and Prior Year Recoveries	504	0	0
Unobligated Balance, End of Year	-1,082	-167	0
Total Court of International Trade (non-EPA)	613	915	167
Court Security			
Unobligated Balance, Start of Year	56	101	0
New Deposits and Prior Year Recoveries	45	0	0
Unobligated Balance, End of Year	-101	0	0
Total Court Security	0	101	0
Federal Judicial Center			
Unobligated Balance, Start of Year	824	974	724
New Deposits and Prior Year Recoveries	150	0	0
Unobligated Balance, End of Year	-974	-724	-724
Total Federal Judicial Center	0	250	0
U.S. Sentencing Commission			
Unobligated Balance, Start of Year	1,669	1,669	0
New Deposits and Prior Year Recoveries	0	0	0
Unobligated Balance, End of Year	-1,669	0	0
Total U.S. Sentencing Commission	0	1,669	0
GRAND TOTAL JTF	\$648,275	\$852,190	\$837,080

**Table 11.2 Judiciary Information Technology Fund
Obligations by Budget Object Class (\$000)**

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

	FY 2021	FY 2022	FY 2023
1100 Personnel compensation	532	699	687
1200 Personnel benefits	3,483	4,579	4,497
2100 Travel	964	1,267	1,245
2200 Transportation of things	1	1	1
2300 Communications, utilities & miscellaneous	75,943	99,831	98,061
2400 Printing and reproduction	4,954	6,512	6,397
2500 Other services	394,346	518,388	509,196
2600 Supplies and materials	7,538	9,909	9,733
3100 Equipment	160,514	211,004	207,262
Total Obligations	648,275	852,190	837,080

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

	FY 2021 Actual	FY 2022 Assumed Obligations	FY 2023 Request
Direct obligations incurred	648,275	852,190	837,080
Obligated balance, start of year	365,136	348,136	624,681
Adjustments of prior year activity	(12,297)	0	0
Obligated balance, end of year	<u>(348,136)</u>	<u>(624,681)</u>	<u>(775,840)</u>
Total Outlays	652,978	575,645	685,921
Less Offsets	<u>(215)</u>	<u>0</u>	<u>0</u>
Net Outlays	652,763	575,645	685,921

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/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 number 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.

COVID-19

The judiciary adjusted quickly to a remote work environment due to the COVID-19 pandemic and took steps to strengthen IT infrastructure to address the increased use of technology for remote work and remote court proceedings. These efforts included increasing the judiciary's bandwidth to meet the additional demand for remote capabilities. The judiciary also acquired additional licenses for technology solutions needed to support remote operations, adjusted the judiciary's video storage retention policy to

support additional capacity, upgraded bandwidth at 175 court locations to address higher network demands associated with remote hearings, and implemented additional functionality for Microsoft Teams to support meetings and collaboration.

IT Infrastructure

The combination of sharp increases in cyberattacks on judiciary IT systems and aging legacy applications critical to court operations has created IT vulnerabilities that require additional resources. Not addressing these IT vulnerabilities will impact the judiciary's ability to provide core IT services and cyber protections for the courts, or to undertake much needed modernization projects.

The American Rescue Plan Act (P.L. 117-2), passed in March 2021, appropriated \$1.0 billion to GSA's Technology Modernization Fund for federal cybersecurity and IT modernization efforts, but this fund is available only to executive branch entities. Other recently enacted investments in cybersecurity and IT modernization, such as significant new appropriations to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), have also been focused on executive branch requirements and priorities to the exclusion of the judiciary. As an independent branch of government with its own significant needs and concerns, the judiciary requires a similarly focused broad investment, tailored to its requirements and business practices, to address the IT infrastructure of the courts and federal defender offices.

In July 2021, the judiciary transmitted to Congress an infrastructure request totaling \$1.54 billion for consideration as part of an ongoing infrastructure reconciliation process. The request included \$515.0 million for cybersecurity and IT modernization, including funding to support cybersecurity improvements to respond to increasing threats and attacks against judiciary IT systems; a range of IT initiatives related to application modernization, network management modernization, and data security modernization; and funding to relocate one of the judiciary's data centers to another location due to a forced move. The request assumed the IT funds would be obligated over four fiscal years. Unfortunately, no iteration of the reconciliation package drafted to date has included any portion of the judiciary's request. As a result, the judiciary has been forced to begin integrating these unmet requirements into its annual budget request. \$20.8 million of these IT-related requirements were included in the judiciary's FY 2022 fall re-estimate, and an additional \$32.4 million was addressed through an intra-judiciary transfer request the Appropriations Committees approved last year; however, the majority of the requirements remain unfunded. The FY 2023 JITF request includes an additional \$80 million related to these IT infrastructure requirements in the sections discussed below, including investments related to cybersecurity, IT modernization, and the move of one of the judiciary's data centers.

Cybersecurity

Like other commercial and government entities, the judiciary is subject to frequent cyberattacks. These attacks have increased significantly over the last several years. Judiciary cyber-defenses blocked more than 43 million harmful events from reaching court local area networks in 2020. This nearly doubles the 24 million attacks blocked in 2019. These incidents target a range of critical areas, including core business functions, relationships with trusted partners, and key security functions such as multi-factor authentication. Though most attacks were successfully thwarted, some incidents caused actual damage, such as localized ransomware infections, payroll redirects, and web page defacements.

These cyberattacks are increasing not only in frequency but also in sophistication as criminal and nation-state bad actors continuously look for new ways to penetrate judiciary networks. As a result of the SolarWinds cyberattack, the judiciary requested an IT security assessment be conducted by CISA. The results highlighted several serious judiciary cybersecurity vulnerabilities that, collectively, pose significant threats to the security and integrity of judiciary IT systems. The judiciary's cyber-defenses must be strengthened to address these vulnerabilities and confront growing threats.

Since implementing a more robust cybersecurity strategy in 2016, the judiciary has initiated significant upgrades and expansions to its cybersecurity operations and continually strengthened its cybersecurity posture. Sustaining these efforts and implementing additional security-related initiatives continues to require substantial resources. The judiciary's data communication network and its underlying infrastructure are ongoing targets of cyberattacks. Sophisticated attackers seek to exploit vulnerabilities and continually develop new capabilities to compromise judiciary information and disrupt, destroy, or threaten the delivery of essential services.

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. At the local court level, court units receive enterprise-license security software for endpoint protection, web-based threat protection, and vulnerability scanning.

For FY 2023, the judiciary requests \$102.5 million in appropriated S&E funding for cybersecurity, which represents an increase of \$5.0 million above the FY 2022 assumed level of \$97.5 million. (This number represents the subset of judiciary IT activities that meets 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. 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.) These resources will be used to support ongoing cybersecurity initiatives as well as new requirements. For example, insider threats are a grave risk to the confidentiality and integrity of judiciary data due to the individuals' current access to judiciary systems, data, and premises. In FY 2023, the judiciary will use dedicated resources ("Red Teams") to create an insider threat program, which will identify and document repeatable processes and procure technologies that support cybersecurity program implementation (ex. Multi Factor Authentication, National Active Directory, Identity Access Management). Red Teams will help identify and assess potential cyber vulnerabilities so that the judiciary can effectively address them.

Second, the judiciary plans to create an IT Security Officer (ISO) Service to allow the AO to appoint a dedicated ISO for each system within the judiciary's national IT portfolio. Many AO offices and programs do not have ISOs designated for the systems they own. Without ISOs, judiciary systems will continue to struggle with security and put the judiciary at a much higher risk level. Additional ISO support for system security packages will also be included as part of the existing National System Security Assessment service that provides comprehensive evaluation of the security posture of national information technology applications.

In addition, the FY 2023 request includes 27 additional positions to support the judiciary's cybersecurity efforts. These positions will support court unit IT security assessment services, ISO services, Red Teams, advanced cybersecurity training, and additional cybersecurity improvements.

Cybersecurity costs are separately presented in table 11.4 on page 11.10 to provide information detailing the judiciary's financial commitment to cybersecurity. (Additional cybersecurity funds are included, but not displayed separately, in the budget accounts for the CAFC, the CIT, the USSC, the FJC, the AO, Defender Services, and Court Security). Within the courts' S&E account, cybersecurity accounts for nearly 16 percent of the total FY 2023 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)

IT Program Component (\$000)	FY 2022 Planned	FY 2023 Request	Increase/(Decrease) From FY 2022
Judicial Statistics & Reporting Systems	212	267	55
Administrative & Management Systems	624	720	96
Telecommunications Program	36,000	40,530	4,530
Infrastructure & Collaboration Tools	59,109	60,367	1,258
Court Administration & Case Management	1,532	618	(914)
TOTAL, S&E JITF Cybersecurity	97,477	102,502	5,025

The FY 2023 S&E JITF cybersecurity request includes adjustments as follows:

- A \$0.2 million inflationary increase in Judicial Statistics and Reporting Systems and Administrative and Management Systems components.
- A \$4.5 million increase in the Telecommunications program is associated with cyclical replacements and upgrades of cybersecurity hardware and software (\$2.6 million), data communication network monitoring devices (\$1.0 million), and operations and maintenance of the national logging service (\$0.9 million).
- A net increase of \$1.3 million in the Infrastructure and Collaboration Tools program component will support the implementation of enterprise multi-factor authentication (\$1.0 million) and a team that will test and validate the judiciary’s security program (\$0.3 million).
- A decrease of \$0.9 million in Court Administration and Case Management is associated with non-recurring cybersecurity costs incurred in FY 2022.

Additionally, in FY 2023, the judiciary plans to use \$39.7 million of Electronic Public Access receipts (compared to \$39.3 million in FY 2022) 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 2023 court cybersecurity program of approximately \$142.2 million.

Modernization Efforts

IT modernization efforts are vital to ensuring the judiciary's IT systems and programs are up-to-date and effectively support the work of the courts, and they are components of several of the budget line items discussed in this chapter. Many of the judiciary's applications do not meet current security requirements and several use programming technologies that are or will quickly become obsolete. Due to these issues, numerous applications present significant security vulnerabilities that are exceedingly difficult for the judiciary to overcome or continue to maintain without additional resources. It is necessary to upgrade or replace aging legacy applications with current and secure solutions that support the mission and administrative needs of the judiciary (such as with PACTS 360, discussed below, and eVoucher).

Additionally, with a rise in the frequency of cyberattacks, these application vulnerabilities present easy targets for malicious actors that want to steal judiciary data, hold systems or data for ransom, or conduct other cyberattacks that can severely impact data integrity of these applications.

It is also important for the judiciary to upgrade its IT architecture and enhance and expand Data Communications Network (DCN) segmentation, which will strengthen IT security by protecting against cyberattacks and improve network performance. The judiciary will also use the requested resources to improve the delivery of cloud and data center services. It will provide real-time application failover (allows applications to seamlessly transition from data center to data center when a data center is down) and allow the judiciary to evaluate and strengthen the data center security architecture. Requested resources will also be used to implement a software defined wide-area network (SD-WAN) to enhance the security of the Judiciary's networks and optimize bandwidth use and redundancy.

The judiciary also plans to use JITF resources to develop a data strategy and governance plan that will enable the judiciary to manage and secure its data as an enterprise asset on par with its people, buildings, and technology. It also allows for standardization of data-related applications, services, and security protocols. These data management efforts help address a finding from the CISA assessment that the judiciary should prioritize and complete the overall data categorization and classification efforts currently underway. These IT modernization efforts are integrated into several of the IT program components discussed later in this chapter.

PACTS 360

The Probation and Pretrial Services Automated Case Tracking System (PACTS) is the case management system used by probation and pretrial services offices to manage the supervision and investigation of defendants and offenders. In recent years, the information technology applications supporting the probation and pretrial services (PPS) system have had significant problems with reliability and performance. At the judiciary 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 and slowdowns, which impede the ability of officers and staff to access crucial case file information.

PACTS 360 development is focused on the replacement system for the legacy PACTS suite of applications. The judiciary has undertaken a two-phased approach to address problems with the reliability and performance of PACTS and the related applications. The first step, which has been successful though not a long-term solution, is to stabilize legacy PACTS and existing applications while a replacement system is developed and deployed. The second step is to develop a replacement system (referred to as PACTS 360) for legacy PACTS and ancillary systems.

For the replacement system, the judiciary has developed and begun a multi-year strategy to implement a Software-as-a-Service solution to replace the existing PACTS system. Beginning in 2020, the judiciary issued a series of contract service orders to work on the various components of PACTS 360 development. Thus far, the PACTS 360 project has mainly been funded through carryforward from the initial PACTS investments in FY 2017 (\$11.1 million) and FY 2019 (\$13.4 million) as well as a small base amount of approximately \$3.5 million. As the project moves forward, costs have increased. Additional PACTS 360 development funding was included in the FY 2022 fall re-estimate, and the judiciary's FY 2023 budget request includes \$33.1 million for the continuation of development and implementation activities. The FY 2023 request also includes 3 positions to support the PACTS 360 development and implementation processes. Two of these positions will be responsible for ensuring a robust data management framework for migration from legacy PACTS to PACTS 360. The additional position's duties will include product development, enhancement and modifications to support business and system capabilities.

Assuming the necessary funding is provided, implementation of PACTS 360 is scheduled to be completed in FY 2024. However, if additional funding is not secured, the project will likely be delayed, and the overall costs for implementation are expected to increase. In addition, without a new, reliable system, probation and pretrial services will not have immediate access to the critical data they need

on defendants and offenders. This would jeopardize officer safety, create an increased risk to public safety, and cause delays in providing services to courts and other agencies.

Data Center Move

The judiciary has two internet data centers, located in Ashburn, Virginia and in San Diego, California. The data centers are geographically dispersed to serve the eastern and western halves of the country. In 2018, AT&T, the owner of the two data centers, sold several of their data centers including those at Ashburn and San Diego. The judiciary must move out of the internet data center in San Diego, California by July 2024 and is proceeding with a plan to replace the data center (in a yet-to-be determined location) and move parts of the infrastructure (such as archival storage and public websites) to the cloud. These infrastructure areas have been deemed cloud-ready and will be moved to the cloud at the same time as the migration to the new data center and after a cloud contract is established in 2022. The impending move plan is designed to minimize operational disruptions to the courts.

The judiciary requires substantial resources to complete the data center move, including funding for additional hardware to stand up a new data center and contractual labor to support the move. The FY 2022 fall re-estimate included \$17.9 million to begin these efforts, and the FY 2023 request includes \$12.6 million to continue these efforts. The contracting process for the data center move is underway, so costs could shift depending on the final procurement outcome.

If funding is not received for this initiative, the judiciary would have to operate from a sole hosting center to support the Data Communications Network (DCN) and Wide Area Network (WAN), which creates high operational risk. A cyberattack or other disruption at the sole data center could result in a potential total shutdown of judiciary IT operations.

Technology Associated with New Courthouse Construction

In FY 2016, Congress provided nearly \$1 billion for eleven courthouse construction projects, which included full funding for eight new courthouses and partial funding for a ninth new courthouse on the Courthouse Project Priorities (CPP) list, and funding for new

construction and acquisition of two federal buildings that jointly house courthouses and other federal agencies that were on GSA's long-range plan. In FY 2018, Congress provided \$437 million to fully fund the ninth FY 2016 courthouse project and to construct two additional courthouses. Congress appropriated partial funding in FY 2021 for two more new courthouse projects. Though funding for the construction of courthouses is appropriated directly to GSA, the judiciary requires funding for IT, security, and other space-related infrastructure requirements to ensure that these new courthouses are fully functional and operational as required by the U.S. Courts Design Guide.

The FY 2023 JITF requirements include \$6.3 million for the costs of providing local-area networks, communications infrastructure, and courtroom technology to new courthouse projects. The total of \$6.3 million in FY 2023 requirements reflects a decrease of \$1.6 million from FY 2022 requirements of \$7.9 million.

Judiciary Information Technology Fund Program Requirements

The FY 2023 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 \$577.7 million of base IT requirements are assumed to be funded in FY 2022. This represents the assumed amount that will be deposited in the JITF from the S&E account. The requirements for FY 2023 are \$654.0 million. As shown in table 11.5 on page 11.15, funding for the S&E JITF obligations supports seven program components.

Table 11.5 Salaries and Expenses Obligations – Judiciary Information Technology Fund Program Requirements

(\$000)

<u>IT Program Component</u>	FY 2022 Projected Obligations (Col A)	FY 2021 Slipped Requirements (Col B)	FY 2022 Base Requirements (Col A - Col B)	Change: FY 2022 Adj. Base Requirements to FY 2023 Current Services Requirements	FY 2023 Program Increases	FY 2023 Total Requirements
Judicial Statistics & Reporting Systems	12,859	1,145	11,714	645	0	12,359
Administrative & Management Systems	71,119	3,807	67,312	13,723	3,791	84,826
Telecommunications Program	125,646	8,068	117,578	6,439	0	124,017
Infrastructure and Collaboration Tools	177,201	21,134	156,067	4,280	2,000	162,347
Court IT Allotments	116,006	535	115,471	2,603	0	118,074
Court Administration & Case Management	49,120	15,537	33,583	30,340	0	63,923
Court Support Reimbursable Program	76,004	0	76,004	9,603	2,831	88,438
TOTAL, S&E JITF	627,955	50,226	577,729	67,633	8,622	653,984

This FY 2023 budget request is based on assumed FY 2022 obligations. The FY 2022 assumed funding level of \$577.7 million will be deposited into the JITF from the S&E account. Any changes to FY 2023 requirements due to the final FY 2022 appropriations will be included in the judiciary’s re-estimates of its FY 2023 budget request.

The following sections present FY 2023 requirements for the S&E portion of the JITF. In total, requirements increase from an assumed base level of \$577.7 million in FY 2022 to \$654.0 million in FY 2023. The FY 2023 request includes program increases of \$8.6 million associated with operational support for the internal controls program (\$3.8 million), 30 additional positions for cybersecurity improvements and PACTS360 (\$2.8 million), and judiciary IT standardization (\$2.0 million). The following pages discuss significant changes between the FY 2022 base requirements and the FY 2023 requirements.

Judicial Statistical & Reporting Systems

FY 2023 Requirements: \$12,359,000
Adjustments to Base from Fiscal Year 2022: \$645,000

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.

The base adjustment in this category includes increases of \$0.4 million associated with data security management and governance and \$0.2 million for inflationary adjustments.

Administrative & Management Systems

FY 2023 Requirements: \$84,826,000
Adjustments to Base from Fiscal Year 2022: \$13,723,000
Program Increase: \$3,791,000

This category 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 web sites.

The base adjustment of \$12.4 million will fund minimum requirements for the upkeep of finance and human resources systems such as software license renewals and periodic updates necessitated by legal and policy changes, and \$1.3 million for inflationary adjustments. If not funded, the judiciary will see an overall degradation of support to administrative systems including a potential delay in upgrading the financial disclosure system and other systems.

The \$3.8 million program increase will fund internal controls evaluation software and self-assessment tools for the Internal Controls Evaluation (ICE) system, which is a software application that helps managers evaluate compliance with internal controls requirements and judiciary procurement policies. The funds will be used for system upgrades, help desk support, and training.

Telecommunications Program

FY 2023 Requirements: **\$124,017,000**

Adjustments to Base from Fiscal Year 2022: **\$6,439,000**

This 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.

Included in the \$124.0 million request are base adjustments of \$2.4 million for inflationary adjustments, \$2.1 million to continue judiciary data communication network cybersecurity improvements, \$1.0 million for data communication network monitoring devices, and \$0.9 million for operations and maintenance of the national logging service.

Infrastructure & Collaboration Tools

FY 2023 Requirements: **\$162,347,000**

Adjustments to Base from Fiscal Year 2022: **\$4,280,000**

Program Increase: **\$2,000,000**

This category encompasses building and maintaining a robust, reliable, and resilient judiciary-wide IT infrastructure.

Included are the costs of hardware, software, and IT security associated with the judiciary’s full enterprise hosting and cloud computing services and email and collaboration systems. This category also includes the costs of IT infrastructure for new courthouse construction projects and operating systems’ support, maintenance, testing, and research.

The base adjustment of \$4.3 million in FY 2023 provides funding for IT security operations including security engineering, awareness, assessment, testing, policy development, and vulnerability remediation support (\$0.8 million) and operations and maintenance of national messaging and collaboration systems (\$0.4 million). The request also includes \$3.1 million for inflationary adjustments and a program increase of \$2.0 million to implement IT standardization which includes the enterprise architecture program. This program will develop and publish technical standards, recommendations, and frameworks to ensure lower costs and improve efficiency across judiciary related data applications, services, and security protocols.

Court IT Allotments

FY 2023 Requirements: **\$118,074,000**

Adjustments to Base from Fiscal Year 2022: **\$2,603,000**

These allotted funds 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 is due to inflationary adjustments (\$2.3 million) and higher FY 2023 requirements for IT infrastructure and maintenance expenses (\$0.3 million).

Court Administration & Case Management

FY 2023 Requirements: **\$63,923,000**

Adjustments to Base from Fiscal Year 2022: **\$30,340,000**

This category contains a variety of tools, including Probation and Pretrial Automated Tracking System (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 the system that captures requests for payments to private court-appointed counsel and expert service providers.

The base adjustment is associated with increases in FY 2023 for the continuation of development and implementation of PACTS 360 (\$26.4 million), architecture and security maintenance of eVoucher (\$2.1 million), and support for PACTS legacy application integration to PACTS360 (\$1.1 million). The increase also includes an inflationary adjustment (\$0.7 million).

If additional funding is not received, the judiciary will be unable to upgrade or replace aging legacy applications with current and secure solutions that support the mission and administrative needs of the judiciary. Many of the judiciary's applications do not meet current security requirements and several use programming technologies that are or will quickly become obsolete. These vulnerabilities present easy targets for malicious actors that want to steal judiciary data, hold systems or data for ransom, or conduct other cyberattacks that can severely impact data integrity of these applications.

Court Support Reimbursable Program

FY 2023 Requirements: **\$88,438,000**

Adjustments to Base from Fiscal Year 2022: **\$9,603,000**

Program Increase: **\$2,831,000**

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 2023 budget request for the court support reimbursable program includes \$88.4 million for the salaries, benefits, and related expenses of AO staff that are reimbursed from the S&E account. The net \$12.4 million increase is attributable to \$3.6

million for standard pay and benefit increases for existing reimbursable positions, \$2.5 million for salaries and benefits for contractor insourcing positions, \$1.5 million increase for non-pay inflation, \$2.4 million in adjustments for the operation and maintenance of IT policy, infrastructure support, testing and administrative support services, and \$0.9 million for annualization costs related to 10 IT positions assumed to be funded in FY 2022. The request also includes a program increase of \$2.8 million for 30 positions to support the increase in requirements for cybersecurity improvements (27 positions) and PACTS360 (3 positions).

During FY 2023, the AO intends to begin implementing another phase of contractor insourcing, which will eliminate approximately 33 contractor positions in FY 2023 and insource the work with a like number of new federal employees. Anticipated FY 2023 savings in the S&E account associated with this insourcing is \$1.2 million due to lower compensation for federal workers versus contractors. When insourcing occurs, the costs of these contractor services that are dispersed in the JITF program components decline while costs in the Court Support Reimbursable program component increase. For more on contractor insourcing and the associated savings, please see page 4.50 in the S&E chapter. For more information on contractor insourcing and AO reimbursable positions, please see the AO chapter, page 8.22 and 8.21.

**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

The Court anticipates obligating \$689,000 from the JITF in FY 2023. This amount includes all required cyclical replacement of equipment. Cyclical information technology equipment replacements scheduled for FY 2023 include the court's network printers used by chambers staff and telecommunications devices. The five-year cyclical replacement of the court's desktop computers, including a combination of desktop towers and Virtual Desktop Infrastructure (VDI) clients, will also occur in FY 2023.

Obligations will also include contract services related to Office 365 projects for the Clerk's Office, including Microsoft Dynamics. In addition, the JITF will be used for the annual renewal of software licenses such as Office 365 and the many other software packages integral to Court operations. Finally, IT equipment maintenance expenses will be paid using funds from the JITF.

Court of International Trade

At the beginning of FY 2022, \$1,082,000 was available in carry forward balances from the JITF. The Court is planning to obligate \$915,000 from the JITF in FY 2022 to:

- Purchase additional audio/video technology for use in courtrooms;
- Purchase mobile audio/video carts to enhance videoconferencing capabilities;
- Continue licensing and maintenance of the court's IT hardware and software applications;
- Continue to maintain and support digital systems, data network and voice connections, (VPN), Voice Over Internet Protocol (VOIP) and the (DCN); and
- Purchase computer desktop systems, monitors, laptops, mobile devices, and printers, according to the judiciary's cyclical replacement program and to facilitate videoconferencing needs.

At the beginning of FY 2023, the Court anticipates that \$167,000 will be available in carryforward balances in the JITF. These funds will be used to continue the Court's information technology 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 2022, the AO had \$2,002,195 available in the JITF from deposits that were made in previous fiscal years. In FY 2022, the AO intends to obligate the entire

amount to replace AO personal computers, laptops, printers, and related equipment pursuant to an approximate four-year replacement cycle, as well as copiers, video conference equipment, and software as required. The AO currently does not anticipate an end-of-year balance to be carried forward into FY 2023.

Federal Judicial Center

At the beginning of FY 2022, the FJC had \$974,000 available in the JITF from deposits that were made in previous fiscal years. A total of \$250,000 is planned for obligation in FY 2022 to provide for the estimated costs associated with IT infrastructure, contract services to support maintenance of IT systems and planned life-cycle replacement of various office automation and technology equipment. The FJC assumes an end-of-year carryforward balance of \$724,000. Currently there are no plans to use JITF funds in FY 2023.

U.S. Sentencing Commission

At the beginning of FY 2022, the USSC had \$1,669,000 available in the JITF from deposits that were made in previous fiscal years. This balance is planned for obligation in FY 2022.

Court Security

At the beginning of FY 2022, \$101,000 was available in the JITF account for the Facility Access Card (FAC) project. The FAC project is the judiciary's version of Homeland Security Presidential Directive-12 (HSPD-12), which developed standards for a secure and reliable form of identification (also

known as "smart cards") for federal government employees and contractors. The implementation of the FAC project was completed in FY 2018 and moved into a sustainment phase in FY 2019. No JITF resources are requested for this or any other Court Security project in FY 2023.