STATEMENT OF

HONORABLE MICHAEL Y. SCUDDER, JR.

CIRCUIT JUDGE
UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT
CHAIR
COMMITTEE ON INFORMATION TECHNOLOGY
ON BEHALF OF

THE JUDICIAL CONFERENCE OF THE UNITED STATES

BEFORE THE COMMITTEE ON THE JUDICIARY
SUBCOMITTTE ON COURTS, INTELLECTUAL PROPERTY,
ARTIFICIAL INTELLIGENCE AND THE INTERNET
UNITED STATES HOUSE OF REPRESENTATVIES

"FISCAL ACCOUNTABILITY AND OVERSIGHT OF THE FEDERAL COURTS"

June 24, 2025

Administrative Office of the U.S. Courts, Office of Legislative Affairs
Thurgood Marshall Federal Judiciary Building, Washington, DC 20544
202-502-1700

STATEMENT OF
HONORABLE MICHAEL Y. SCUDDER JR., CHAIR
COMMITTEE ON INFORMATION TECHNOLOGY OF THE
JUDICIAL CONFERENCE OF THE UNITED STATES
BEFORE THE SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY,
ARTIFICIAL INTELLIGENCE, AND THE INTERNET
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

June 24, 2025

INTRODUCTION

Chairman Issa, Ranking Member Johnson, and members of the Subcommittee, my name is Michael Scudder, Jr., and I am pleased to appear before you today as Chair of the Judicial Conference Committee on Information Technology. I look forward to speaking with you about the Judiciary's information technology program. My remarks are meant to complement those of Judge Amy J. St. Eve, Chair of the Judicial Conference Committee on the Budget.

I have served as a judge on the United States Court of Appeals for the Seventh Circuit since 2018. In addition, I have served on the Judiciary's IT Committee since 2019 and as its Chair since 2021. Prior to my judicial service, I served as an attorney in the Executive Branch and in private practice. This is my first appearance before this Subcommittee.

INFORMATION TECHOLOGY PROGRAM

At the outset, I want to observe that IT is critical to everything the Judiciary does. Cases are filed, docketed, and managed electronically. Judges and staff rely on a wide array of IT applications for nearly every aspect of our operations, whether writing an opinion or entering an order, paying an expense, or communicating with colleagues. Looking back over the last couple of decades as technology has changed and advanced, the Judiciary's funding levels have not kept pace to address needed improvements. So the branch found itself in a position of underinvestment in our IT infrastructure and applications. While we have always been responsible stewards of taxpayer dollars, overarching budgetary challenges to maintain current service levels also have limited our investment in IT development and necessary enhancements to the Judiciary's IT infrastructure. Until recently, this underinvestment left our major systems and applications outdated and vulnerable. Many are not up to date with modern development standards or security protocols. The result is that our systems are expensive to operate, update, or replace; difficult to maintain; and at regular risk of either operational failure or security breaches. At the same time, the Judiciary has faced challenges in hiring and retaining trained IT professionals given potential compensation for employment outside of government.

There are two recent issues which have elevated the judiciary's IT needs to the forefront. First, the Judiciary has had to respond to waves of highly sophisticated and persistent cyber threats. Given the information in the Judiciary's control, we continue to face unrelenting

security threats of extraordinary gravity. We expect the risks and potential damages from these attacks will keep intensifying into the indefinite future. Second, as other institutions of government and the private sector experienced in their own ways, the COVID-19 pandemic stressed many of our systems to near breaking points with unprecedented remote access for the public and litigants to court proceedings and exposed many shortcomings and needs.

The Judiciary is committed to investing in IT to keep our IT environment up to modern and operational security standards and thereby able to confront the constant and increasingly sophisticated cybersecurity threats the branch faces.

CYBERSECURITY RISKS

By virtue of the work it performs, the Judiciary possesses extremely sensitive and non-public data. This includes personally identifiable information, confidential sealed documents (including indictments, arrest and search warrants, and cooperator information), national security information, evidence with proprietary economic value, as well as draft opinions and orders, among others. If sensitive information were inappropriately accessed, distributed, or modified, or if the branch's ability to use its systems for the necessary conduct of day-to-day judicial activities were compromised, there could be immediate and significant effects on national security, the economy, community safety, and even confidence in the integrity and strength of the courts and the broader federal government.

These observations are not hypothetical. Experience has shown that the Judiciary is a high-value target for malicious actors and cyber criminals seeking to misappropriate confidential information and disrupt the judicial process in the United States. These attacks pose risks to our entire justice system, including civil and criminal court proceedings, law enforcement and national security investigations planned or underway, and trade and commercial secrets for businesses involved in bankruptcy proceedings or patent and trademark litigation.

We work closely with our Executive Branch partners, including the Department of Justice's National Security Division, Federal Bureau of Investigation cybersecurity experts, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Office of the National Cyber Director, to identify and better understand cyber risks, bolster our cyber defenses, and investigate cyber-attacks that occur on our IT systems. This inter-branch coordination and information and intelligence sharing is critical to addressing comprehensively the cyber challenges facing the federal government as a whole. We are grateful for the outstanding support we have received from the Executive Branch.

To provide some sense of the magnitude of this threat, 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 previous year, although the sophistication of the attacks indicates new approaches are being deployed in attempts to access confidential information and disrupt Judiciary operations. Because of the sensitivity of the information, I am constrained in what I can say in this setting about vulnerabilities and cyber-attacks on the Judicial Branch. With assistance from our Executive Branch partners, we provided a classified briefing for appropriations and authorizing full Committee and Subcommittee leadership in May where we

provided more details about specific incidents that have occurred and their implications. We would be happy to do so again for any member of the Subcommittee.

For the past several years, the Judiciary has been modernizing its cybersecurity operations and strengthening its cybersecurity posture. Many of the projects summarized below will help strengthen the security of the branch's IT systems and applications. We appreciate Congress's understanding and past support of our IT challenges and hope the FY 2026 appropriation will result in ongoing funding for our ongoing initiatives to modernize and better secure our systems.

MAJOR INFORMATION TECHNOLOGY PROJECTS

The Judiciary has several initiatives and programs underway to achieve a secure and modern IT environment. Importantly, for these projects, the Judiciary is committed to a culture of accountability and robust oversight. The branch created a new Chief Information Officer position in 2022 to ensure enterprise oversight and overarching responsibility for all IT projects. Within the CIO's office, project management oversight efforts have dramatically increased with regular internal project reviews and evaluations and reporting regularly to the Judicial Conference IT Committee.

IT Modernization and Cybersecurity Strategy

Cyber breaches we experienced in recent years led to the creation, under the leadership of our former Director, Judge Roslyn Mauskopf, of an IT Security Task Force. The Task Force completed its work in 2023 and produced 25 recommendations, which the IT Committee has been working to address and implement. For its part, the IT Committee developed and produced a comprehensive multi-year (FY 2022 – FY 2027) *IT Modernization and Cybersecurity Strategy* (*Strategy*) in June 2022. That Strategy continues to guide the IT Committee's work and the Judiciary's current Director, Judge Robert Conrad, has continued to make IT modernization and cybersecurity as a top priority of the branch. All of these efforts have helped unify the branch around a common IT strategy and achieving its objectives with urgency—in cyber relevant time frames as we often put it.

IT Modernization and Cybersecurity Strategy Funding

In FY 2022, we began requesting funds pursuant to this multi-year *Strategy*. The Judiciary's FY 2026 funding request includes $74 million of multi-year plan funding for the courts' Salaries and Expenses and the Defender Services accounts. This will allow us to continue making progress towards modernizing the Judiciary's IT systems and strengthening IT security.

With the funding provided so far, we have achieved substantial progress, including the full implementation of multifactor authentication ("two step verification" when logging into an account or system) at every Judiciary workstation; the completion of the first of four phases of a project to move the Judiciary to a new identity credentials program that will reduce reliance on

outdated password-oriented paradigms and allow better control systems and data access; the continued deployment of enhanced network monitoring and activity logging tools, as well as stronger firewalls and endpoint protection tools, on Judiciary systems, applications, and devices.

As Judge St. Eve emphasizes in her testimony, these successes are dependent on the Judiciary's receipt of funding to continue, complete, and sustain these high priority initiatives. We cannot continue absorbing cybersecurity and modernization costs in a flat budget environment without doing unacceptable harm to other critical areas of judicial operations.

Upgrades to the Judiciary's Financial Management System

We are in the process of completing significant upgrades to the Judiciary Integrated Financial Management System (JIFMS), the Judiciary's official budget, accounting, and procurement system. The upgrade is critical to address technical obsolescence of third-party support tools, and security and performance concerns. Recommendations for improvements to internal controls will be addressed with the upgrade, improving both operational and technical efficiencies while strengthening the Judiciary's cybersecurity posture. The upgrade will facilitate compliance with both regulations regarding inter-governmental funds transfers between federal agencies for goods and services procured, as well as future upgrades that will further improve Judiciary financial management. The JIFMS upgrade is in its final stages of implementation, with the project being on time, within scope, and on budget.

Court Case Management System Modernization

The branch's top IT priority is replacing the Judiciary's case management/electronic case filing (CM/ECF) system and its portal, the Public Access to Court Electronic Records (PACER) system. CM/ECF is the backbone system federal courts depend on for mission critical, day-to-day operations. It is used by electronic filers to submit filings in all cases and proceedings, including criminal, civil, appellate, and bankruptcy matters. And it is used by judges and court staff to conduct many tasks related to case management. PACER is the front-end portal to CM/ECF used by individuals, businesses, federal entities, and others to access public court records.

Based on extensive internal and external analyses, we have concluded that CM/ECF and PACER are outdated, unsustainable due to cyber risks, and require replacement. Intensive efforts to modernize these systems are underway. Our 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 versus the past model of implementation only after a system is fully designed, developed, and tested. This "agile" software development and implementation approach is consistent with current industry best practices. At this point in our planning, we hope to incrementally deliver the modernized case management system to pilot courts in the coming fiscal years. At the same time, the judiciary continues to take steps to protect, as best we can, the existing CM/ECF and PACER systems to reduce cyber risk while the new case management system is being developed.

Recent Congresses have considered legislation related to CM/ECF and PACER modernization, including the timing and technical requirements of a modernized system and changes to the structure of PACER user fees. The Judiciary is fully committed to CM/ECF and PACER modernization as well as to continued broad public access to court records. We have no preference for PACER user fees as the funding source for CM/ECF and PACER; however, it is critical that there is an adequate, stable, and predictable funding stream to enable us to modernize and operate the systems on a going forward basis.

We will continue to keep the Subcommittee apprised as to the progress of our CM/ECF and PACER modernization efforts, as well as the impact of any legislation that changes the current PACER fee structure on our ability to finance CM/ECF and PACER activities.

Modernizing the Probation/Pretrial Services Case Management System

The Probation and Pretrial Services Automated Case Tracking System (PACTS) is used by approximately 8,000 probation and pretrial services officers and staff to conduct and manage investigations, risk assessments, and supervision of defendants and individuals on pretrial or post-conviction release. The current system relies on approximately 30 separate IT applications to enable probation and pretrial services offices to perform their official duties. The complexity of integrating so many applications has resulted in recurring outages, slowdowns over many years, and increasing costs to maintain an outdated system architecture. We have taken steps to stabilize the current system while we develop a new one, which we are calling PACTS360. PACTS360 is a cloud-based application that will modernize system architecture, strengthen cybersecurity defenses, and improve system functionality and reliability for probation and pretrial services officers. Based on substantial progress in recent years, we currently expect PACTS360 implementation in all probation/pretrial services offices nationwide to be completed by the end of FY 2027.

Artificial Intelligence

The rapid proliferation of Artificial Intelligence (AI) tools in everyday life has magnified AI's implications for the Judiciary. While AI has the potential to improve productivity in court operations, create more efficient ways to engage with the public, and support judicial decision making, the use of AI also poses privacy, security, and other risks that must be considered. In January 2025, the AO Director established an AI Task Force to serve a central coordinating role within the branch on AI issues. The task force comprises judges and Judiciary personnel to ensure broad representation in considering AI-related issues on Judiciary operations. The goal of the task force is to balance the Judiciary's ongoing pursuit of leveraging cutting-edge technologies to improve operations and create efficiencies, with the need to address very real privacy and security issues presented by AI. It is currently envisioned that this task force will complete its work by December 2026.

CONCLUSION

Chairman Issa, Ranking Member Johnson, and members of the Subcommittee, thank you again for the opportunity to testify today. I would be pleased to answer your questions.