JUDICIAL CONFERENCE OF THE UNITED STATES

WASHINGTON, D.C. 20544

THE CHIEF JUSTICE
OF THE UNITED STATES
Presiding

HONORABLE ROBERT J. CONRAD, JR.
Secretary

August 7, 2025

Honorable Jim Jordan
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Enclosed, please find responses from the Judicial Conference of the United States to questions for the record submitted by House Judiciary Committee members following the June 24, 2025, hearing entitled "Fiscal Accountability and Oversight of the Federal Courts."

If we may be of further assistance to you in this or any other matter, please contact the Office of Legislative Affairs, Administrative Office of the United States Courts, at (202) 502-1700.

Sincerely,

Robert J. Conrad, Jr.
Secretary

Enclosure

cc: Honorable Jamie Raskin

Questions for the Record from Representative Darrell Issa for the Honorable Amy St. Eve
Fiscal Accountability and Oversight of the Federal Courts
June 24, 2025

---

1. ***Please clarify the dollar amount and proportion of the $800 million requested budget increase that is earmarked for physical security and do the same for cybersecurity.***

   Answer: Of the $800 million of discretionary appropriations increases requested across the branch as part of the FY 2026 budget process, $173 million, or 22%, is directly tied to physical security needs. Of that $173 million, $30 million is for base adjustments for ongoing physical security activities, and $143 million is for necessary security enhancements.

   The proportion of the budget request that is dedicated to cybersecurity varies depending on the precise definition of cybersecurity being employed. Approximately $69 million (9%) of the branch-wide requested increase is associated with direct information technology (IT) security activities or the upgrade, replacement, or sustainment of systems and other IT infrastructure with substantial vulnerabilities that can be mitigated through additional investment, such as modernization. (Note that these numbers do not include the significant costs associated with the modernization and security enhancements of the Case Management/Electronic Case Files system, which are paid for with non-appropriated funding via Electronic Public Access user fees.) Of the $69 million, $43 million is for base adjustments for ongoing activities and $26 million is for enhancements.

   The remaining resources requested as part of the $800 million and not enumerated above are necessary primarily to sustain current operational levels (for example, increases in the rent charged to the Judiciary by the General Services Administration or changes to benefit rates as calculated by the Office of Personnel Management) or to redress the significant funding shortfall that exists in the Defender Services panel attorney program as a result of the full year continuing resolution in FY 2025. Many of these expenses are not optional and, if not appropriately funded, will substantially erode the funding that remains for basic judicial services.

2. ***Please identify specific subcategories or line items in the Judicial Branch's budget request that represent unnecessary redundancies or correspond to areas where further economizing is possible.***

   Answer: The Judiciary carefully reviews its budget prior to submission to ensure that each dollar requested is for a discrete and necessary purpose. As a result, there are no subcategories or line items in the Judiciary's request that represent redundancies.

   With respect to possibilities for further economizing, the Judiciary has a longstanding and active cost containment program with the intended purpose of identifying and acting on such possibilities. In fact, the Judicial Conference's Budget Committee has an Economy Subcommittee that, as its name suggests, exists specifically to look for economies to streamline the Judiciary's operations and reduce cost growth in its budget. The history

and status of the cost containment program was discussed in detail in Judge St. Eve's written statement to the Subcommittee, as well as in the Judiciary's annual budget justification materials submitted to Congress (see, for example, the "Cost Containment" sections on pages 4.22 – 4.24 and 5.18 – 5.22 of the FY 2026 Congressional Budget Request). The Judiciary routinely includes reductions in its budget requests associated with economizing measures implemented through its cost containment program and will continue to do so when appropriate. Such measures, however, require careful planning to ensure their successful and responsible implementation and to avoid a resulting negative impact on the quality of Judiciary services. As such, there currently are no subcategories or line items in the Judiciary's pending budget request that represent areas where further economizing is immediately possible, however, the Judiciary continually reviews its programs and spending to identify where additional efficiencies and cost savings can be achieved.

3. ***With respect to physical security specifically, what can be done to streamline administratively between court security officers employed by the courts, the U.S. Marshals Service, and other aspects of the courts' security setup, so that there is a single point of accountability for ensuring the safety of judges, staff, and the public, while reducing overhead?***

Answer: Judicial security is a complex, multilayered program with services being rendered by three executive branch agencies: 1) the U.S. Marshals Service (USMS); 2) the Federal Protective Service (FPS); and 3) the General Services Administration (GSA). USMS is statutorily the primary agency charged with the protection of the Judiciary (28 U.S.C. § 566), and is responsible for the protection of federal judges, court employees, witnesses, and other threatened persons where criminal intimidation impedes on the functioning of the judicial process or any other official proceeding. The geographical structure of the USMS mirrors the structure of United States district courts. There are 94 federal judicial districts, including at least one district in each state, the District of Columbia, the Commonwealths of Puerto Rico, and the Northern Mariana Islands and the two territories of the United States – the Virgin Islands and Guam. Its responsibilities include:

1. Ensuring that courthouses and its occupants are safe; and

2. Providing personal security for federal judges, including government-funded residential security systems to secure judges' homes.

3. Managing the Court Security Officer (CSO) program.

CSOs are not federal employees. Instead, a private security company under contract to the USMS employs them. The Judiciary provides full funding for the CSO program through the annual Court Security Appropriation (CSA). CSOs are deputized as Special Deputy U.S. Marshals (in effect only while they are on-duty) and wear a USMS insignia on their blazers. The USMS Judicial Security Inspector (JSI) is the Contracting Officer's

Representative (COR) for the district's CSO program and is responsible for ensuring that the vendor provides and staffs the CSOs in accordance with USMS guidelines.

The Director of the USMS retains final authority on judicial security requirements but regularly consults with the Judicial Conference of the United States, through its Committee on Judicial Security, on the security needs of the federal Judiciary.

FPS is responsible for the physical security of all federal buildings owned or leased by GSA (Pub. L. No. 107-296), including courthouses and multi-tenant facilities housing court and court-related operations. This responsibility overlaps with that of the USMS regarding Judiciary facilities. To clarify the appropriate division of responsibility among these agencies, memoranda of agreement (MOAs) have been executed by the Administrative Office of the U.S. Courts (AO), USMS, GSA, and FPS. Under these MOAs, the USMS has responsibility for the security of Judiciary areas within GSA-owned, leased, and/or managed buildings, and FPS has the primary responsibility for law enforcement-related duties and perimeter security at these locations, on a reimbursable funding basis.

The AO's Judiciary Security Division (JSD) serves as the primary representative in dealings between the Judiciary, USMS, FPS, GSA, and other agencies on court and judicial security matters. JSD provides security advice and assistance to the federal courts, formulates and executes security policies for the Judiciary, monitors the USMS's implementation of the Judicial Facility Security Program, and aids the courts on security related issues and trainings. JSD also oversees the AO and Judiciary Emergency Management program, providing advice and assistance to the courts on Emergency Management, Crisis Response, Occupant Emergency Plans (OEP), and Continuity of Operations Planning (COOP). JSD provides staff support to the Committee on Judicial Security and is funded directly through the CSA and is responsible for the oversight and management of CSA funding as determined by the JSC.

4. ***You acknowledged that the budget request does not capture expenditures spent on judicial conduct and disability investigations and compliance, such as in the case of Judge Pauline Newman. Please provide more specific information on the use of appropriated funds for such purposes.***

Answer: In general, funding for investigating Judicial Conduct and Disability (JC&D) matters comes from the Salaries and Expenses (S&E) Appropriation within the Court of Appeals, District Courts, and Other Judicial Programs.

The AO Director may authorize expenses of circuit judicial councils in JC&D matters under 28 U.S.C. § 604(h)(1) from the S&E Appropriation Account. Courts do not always seek funding from the AO Director to procure the services of outside experts, investigators, or medical experts in JC&D matters. Some complaints are investigated by the judges on the special committee (28 U.S.C. 353(a)(1)) with assistance from Judiciary staff resulting in very little expense other than salaries of staff already on board.

Additionally, where a complaint involving a special committee investigation is dismissed, the circuit judicial council can recommend that the Director of the AO reimburse reasonable expenses of the subject judge, including attorneys' fees. *See* 28 U.S.C. § 361. Generally, these reimbursements are derived from the S&E Appropriation.

When the Judiciary is sued in relation to a JC&D complaint, the Department of Justice (DOJ) generally represents the Judiciary. Expenses associated with DOJ's representation of the Judiciary are covered by appropriations available to DOJ. When DOJ representation is unavailable, the AO Director may authorize funding from the court S&E appropriation to pay for legal representation as appropriate.

Each circuit devotes staff time to processing JC&D complaints. The number of FTEs performing this work varies by circuit. A considerable portion of this activity involves processing complaints from litigants that are ultimately dismissed as directly related to the merits of a judge's decision.

Congress appropriates a separate appropriation to the Federal Circuit for the operations of that court, including JC&D matters that arise in that court. Generally, the Federal Circuit's expenditures are not subject to the discretion of the AO Director or the Judicial Conference of the United States. Accordingly, expenses of investigations authorized by that Circuit would come from the Federal Circuit Court of Appeals Appropriation.

5. ***What oversight mechanisms does the Judicial Branch use to ensure that appropriated funds – such as funds apportioned to community defender organizations– are not used for ideologically or politically biased purposes, or other improper purposes?***

Answer: The Judicial Branch has extensive guidance for Judiciary personnel on ethics matters, including on political activity generally and a prohibition on using appropriated funds for political activity.

The Judiciary has a robust audit program in place. Financial statement audits of courts and federal public defender offices (FPDOs) are conducted on a cyclical basis, and audits of Community Defender Organizations (CDO) are performed annually. All financial statement audits are designed to determine the proper use of allocated funds to courts and FPDOs and grants funds awarded to CDOs. Instances of improper use of funds that are identified would result in an audit finding requiring corrective action.

In addition, Judiciary employees are encouraged to report suspected fraud, waste, or abuse, with multiple channels available for reporting. For example, an allegation of suspected wrongdoing in a district court may be reported to that district's clerk of court, chief judge, the circuit executive, or the AO. Credible claims of waste, fraud, and abuse are thoroughly investigated, and the outcomes of investigations must be reported to the AO. The Judicial Conference Committee on Audits and AO Accountability is briefed on all investigations and outcomes.

Regarding CDOs specifically, CDOs are grant funded organizations that provide representation to eligible federal defendants under the Criminal Justice Act (CJA). CDO grant conditions limit the use of grant funds solely for the purpose of providing representation and other appropriate services in accordance with the CJA and the CJA Guidelines (contained in Guide to Judiciary Policy, Vol. 7A). Additionally, as noted above, CDOs are subject to annual audits contracted by AO. The AO's Defender Services Office also reviews CDO monthly accounting reports for any unallowable expenses.

Furthermore, the grant conditions require adoption of a Code of Conduct. Canon 7 of the Code provides that CDO employees should not engage in any political activity while on duty or in the CDO workplace and may not utilize any federal resources in any such activity. A CDO employee may engage in political activity not otherwise prohibited, provided it does not detract from the dignity of the office or interfere with the proper performance of official duties. A CDO employee who participates in political activity should not use his or her position or title in connection with such activity. Similar policies are in place for FPDO employees.

6. ***What proportion of "salary and expenses" costs goes to maintaining or upgrading case assignment systems and procedures, and are there any plans to change those systems or procedures across the judiciary?***

Answer: The Judiciary does not centrally track costs associated with courts' case assignment systems. The Judicial Conference is not considering proposals to change its longstanding policies in support of random case assignment. Although the Judiciary is in the process of updating its Case Management/Electronic Case Files system, known as CM/ECF, the functionality that will be built to support case assignment will comply with the Judicial Conference's random case assignment policy. Moreover, any such functionality must account for the critical role that individual courts have in crafting and effectuating their local case assignment plans. Congress has vested courts with the authority and flexibility necessary to provide for the division of work among their judges. As recognized in this statutory scheme, courts, not the Judicial Conference, are in the best position to determine the most effective means of managing and balancing their business, while promoting random assignment and ensuring the efficient administration of justice.

7. ***In the wake of the recent Supreme Court decision in Trump v. CASA, Inc., what expenditures do you expect will be made by courts to certify, whether provisionally or otherwise, nation-wide classes under Rule 23 of the Federal Rules of Civil Procedure to permit injunctions against the federal government with nation-wide scope to remain in place notwithstanding the Supreme Court's decision?***

Answer: Given the recentness of the *Trump v. CASA, Inc*., 606 U.S. ___ (2025), 145 S. Ct. 2540 decision, we do not yet have sufficient data to evaluate what expenditures might result from a change in litigant behavior in response to the decision. To the extent that

courts have granted injunctions that are broader than necessary to provide complete relief to each plaintiff with standing to sue, it is possible that affected litigants might, instead, file a separate or amended complaint on behalf of a purported class in an attempt to obtain relief with a similarly broad scope. Litigants seeking relief under Federal Rule of Civil Procedure 23 must meet the very specific standards of the rule and related case law to be granted class certification. A court is limited to certifying classes that meet those requirements. Depending on the type of class action, that determination could require appointment of interim class counsel, preliminary discovery, and an assessment of common questions of law and fact. In an exception to the general rule that appellate review must await a final judgment, a party may file a petition for a court of appeals to review a class certification order in an interlocutory appeal. The court of appeals has discretion on whether to take the appeal of a district court's class certification decision.

Once a court has certified a class, class action litigation requires substantial judicial consideration, including oversight of proposed settlement agreements. Moreover, any request for class-wide injunctive relief must carefully account for the equities of the class, rather than a small number of individual plaintiffs. Because of the potential for irreparable harm when injunctive relief is at issue, orders granting, modifying, dissolving, or refusing injunctive relief are subject to an immediate appeal as of right. In short, injunctive relief in class actions is not granted lightly and is subject to robust interlocutory appellate review.

8. ***What expenditures do you expect would be needed for the Judicial Conference to enact rules or guidance for the courts to require compliance with Rule 65(c) of the Federal Rules of Civil Procedure—specifically the requirement to impose an adequate security— in every preliminary injunction or temporary restraining order decision?***

Answer: An estimate of the expenditures necessary for the development of any possible additional rules or guidance related to this issue cannot be developed at this time. The Judiciary is still assessing the interrelated impacts of the Supreme Court's June 27, 2025 decision in *Trump v. CASA, Inc.*, 606 U.S. ___ (2025), 145 S.Ct. 2540, related recent Executive Orders, and presidential memoranda. This assessment will also help determine if any changes are necessary regarding current compliance by courts and parties with Federal Rule of Civil Procedure 65(c) and existing procedures used by federal district court clerks' offices to support compliance with this rule.

1. ***This Subcommittee is concerned about inadequate protections for trade secrets and confidential business information in litigation due to the involvement of bad actors, including those sponsored by adversary nations. Such bad actors may become involved through third party litigation funding, for example. Is the Judicial Branch examining ways to detect such bad actors and address concerns about improper disclosures of confidential information, whether through new rules or improvements to the courts' systems?***

    a. ***[Follow-up]: Is there any technology, including emerging technologies like AI and blockchain, that the Judicial Branch is exploring to help prevent bad faith litigants or other bad actors from exploiting our judicial system to steal valuable information from U.S. companies?***

Answer: The Judiciary is sensitive to concerns of malpractice and misuse of the judicial system. The Advisory Committee on Civil Rules has received several suggestions related to third-party litigation funding, and a subcommittee has been formed to monitor and study the issue. However, there are no plans for any proposals for rule amendments in the near future because it takes time to understand the implications of new rules and to obtain input from all the relevant constituencies. As a general matter, the judge assigned to a case is responsible for policing the parties and the attorneys appearing before him or her. The presiding judge is also in the best position to identify and address the concern that bad actors might be facilitating or financing particular litigation in an effort to obtain trade secrets and confidential business information. In jurisdictions where judges or courts have concerns based on their caseload, they have discretion to issue standing orders or local rules that require additional disclosures related to third party litigation financing.[1] Indeed, some district courts have adopted local rules or standing orders with regard to the disclosure of funding.

Moreover, judges have a wide array of options that can be tailored to the circumstances of a particular case. For example, judges can issue protective orders that restrict the dissemination of discoverable material. When monitoring and enforcing their orders, judges have considerable discretion in crafting appropriate sanctions, including fines, limiting the admission of evidence, and, in more extreme cases of bad faith, civil contempt and even the dismissal of the lawsuit.

In addition, the Judiciary is constantly exploring and implementing various solutions and measures to safeguard its systems. A few examples of safeguards the Judiciary has in place to help prevent bad faith litigants or other bad actors from exploiting our judicial system to steal valuable information from U.S. companies include the following: data encryption for data at rest and in transit; multi-factor authentication being used to access the applications and network; continuous monitoring; and intrusion detection and

[1] *See, e.g.*, Standing Order Regarding Third-Party Litigation Funding Arrangements (D. Del. Apr. 18, 2022) (Connolly, C.J.); N.D. Cal. Civ. L.R. 3-15(b)(2) (requiring disclosures related to nonparties).

prevention.

We leverage Artificial Intelligence / Machine Learning to strengthen our cybersecurity posture, by applying the techniques to improve how we monitor data and identify potential issues across the Judiciary. This includes looking for unusual patterns or behaviors that might indicate a risk to our systems or data.

Questions for the Record from Representative Darrell Issa for the Honorable Michael Scudder, Fiscal Accountability and Oversight of the Federal Courts
June 24, 2025

---

1. ***How are particular IT and cybersecurity needs identified, and what methodology is used to determine how to spend funds to address those needs?***

   Answer: The Judiciary identifies IT and cybersecurity requirements throughout the lifecycle of its IT systems from initial design and development through operations and maintenance. The Judiciary also continuously assesses the threat environment against newly identified vulnerabilities to mitigate risk and remediate weaknesses before they can be exploited. This is done proactively through routine scanning, penetration testing and red teaming (team simulating real world cyberattack) of Judiciary IT systems and processes and reactively following the detection of new vulnerabilities or in response to security events and incidents.

   The Judiciary's broad IT and cybersecurity needs are identified in certain planning and strategy documents. The Judiciary's Long-Range Plan for Information Technology is updated on an annual basis and generally describes key strategic priorities. In recent years, and as noted in Judge Scudder's written testimony, the Judiciary created an IT Security Task Force that produced 25 recommendations which the Judiciary is actively implementing. Relatedly, the Judiciary developed a comprehensive multi-year (FY 2022 – FY 2027) IT Modernization and Cybersecurity Strategy, and the Judiciary requested appropriated funds since FY 2022 to implement this Strategy.

   Finally, the Judiciary has a robust process for requesting and obligating funds to address these identified needs. All IT and cybersecurity requirements are closely scrutinized in the Judiciary's annual budget formulation process. These requirements also undergo analysis by the Chief Information Officer, a host of internal governance groups, the Judicial Conference's Committee on Information Technology, the Judicial Conference's Committee on the Budget (and other Judicial Conference committees), and, ultimately, the Judicial Conference itself for inclusion in the Judiciary's annual budget request. In terms of obligating and spending funds, the Judiciary develops an annual financial plan detailing IT and cybersecurity needs and projects. IT services are closely monitored each fiscal year with regular reporting, project management oversight, and regular formal project review meetings.

2. ***Will the Judicial Conference and Administrative Office of the United States Courts work with Congress to explore a modernization overhaul of the PACER and CM/ECF systems, including with respect to evaluating potential private-sector solutions, expanding free access for the public, and improving financial accountability?***

   Answer: As noted in Judge Scudder's written testimony, the Judiciary's top IT priority is replacing its case management/electronic case filing (CM/ECF) system and its portal, the Public Access to Court Electronic Records (PACER) system. 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 already underway. The Judiciary remains committed to the modernization effort and has considered a range of possible solutions, including from the private sector. The Judiciary will balance costs and the expeditious rollout and implementation of the modernized system as well as ensuring the relevant internal and external stakeholders can provide their input to account for the Judiciary's business needs. The Judiciary has provided and will continue to provide updates to Congress on this important priority.

The Judiciary also remains committed to continued broad public access to court records. Approximately 84 percent of active PACER users qualified for a fee waiver in FY 2024 and were, therefore, able to access court records for free. Of the remaining users who do incur fees, many are high-volume commercial users, some of which monetize or otherwise recoup the costs of data accessed from PACER as the foundation of their own business models. As noted in Judge Scudder's written testimony, 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. It is critical that the Judiciary continue to receive a sufficient, predictable funding stream to ensure we can modernize, operate, and continuously improve the systems to meet the dynamic changes in technology, Judiciary business needs, security, and statutory requirements. If PACER fees are eliminated, the Judiciary would need a significant amount of appropriated funds to replace that revenue to fund operation of the current system and the modernization effort or would otherwise be forced to reduce or eliminate investments in new public access technologies and reduce existing public access services.

3. ***Given the current operational environment and the state of the courts' cybersecurity measures, what risks exist for litigants who have proprietary or other confidential information on court IT systems, including information under seal?***

Answer: Similar to all public sector and private sector organizations, the Judiciary is constantly attacked by malicious cyber actors at the rate of over 11 million potential attempts daily. Risks for litigants who have proprietary or other confidential information on our court IT systems, including information under seal, are real. The risks facing individuals impacted by cybersecurity incidents is a driving force in the Judiciary's efforts to address vulnerabilities and modernize our systems. Though the risks cover a large spectrum in terms of context and severity, the Judiciary is working diligently to find all possible ways to mitigate risk. This includes working closely with the Executive Branch. At the same time, the Judiciary has undertaken (and continues to undertake) measures to protect confidential information, including, in particular, sealed documents. The Judiciary constantly seeks to strengthen these measures, and some of its legacy systems necessitate modernization efforts to defend against more advanced and sophisticated techniques by cyber threat actors.

As was noted in Judge Scudder's written testimony, we provided a classified briefing for appropriations and authorizing full Committee and Subcommittee leadership in May where we relayed 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.

4. ***What cybersecurity risks or other risks (e.g., ethical or legal risks) are presented when third party entities with significant direct interests in a case, such as a litigation funding or investment entity, are not disclosed to the judge?***

Answer: We are not aware of elevated cybersecurity risks related to third party litigation at this time. Under the Code of Conduct for United States Judges, federal judges have an obligation to "maintain and enforce high standards of conduct and should personally observe those standards, so that the integrity and independence of the judiciary may be preserved." Canon 1.

As the GAO noted in its December 2024 report [1] on third-party funding of patent litigation, "[w]hether a judge's investment in a third-party funder would require recusal depends on if such an investment 'could be affected substantially by the outcome of the proceeding.'"

[1] GAO Report is available at https://www.gao.gov/assets/gao-25-107214.pdf.

Questions for the Record from Representative Scott Fitzgerald for the Honorable Michael Scudder, Fiscal Accountability and Oversight of the Federal Courts
June 24, 2025

---

1. ***You state in your testimony that the Judiciary "work[s] closely with our Executive Branch partners, including the Department of Justice's National Security Division, FBI, the Department of Homeland Security, and the Office of the National Cyber Director, to identify and better understand cyber risks, bolster cyber defenses, and investigate cyber- attacks that occur on our IT systems." Do you utilize interagency coordination for physical security assessments as well? For example, would the Courts ask the FBI or Secret Service to examine its security to better understand and assess gaps or vulnerabilities? And if not, why not?***

   Answer: With regards to physical security, we routinely coordinate with Executive Branch security partners—e.g., the U.S. Marshals Service (USMS) and the Federal Protective Service (FPS)—as well as national, state, and local law enforcement and public safety agencies to collaboratively assess potential Judiciary vulnerabilities. This includes collaboration with the U.S. Secret Service, Federal Bureau of Investigation, state fusion centers, and local police departments (e.g., U.S. Capitol Police, D.C. Metropolitan Police, New York Police Department, and others) regarding potential risks and vulnerabilities associated with global or local issues (e.g., sovereign citizens, fraudulent jury summons, national security special events, and Special Event Assessment Rating events,) to better inform long- and short-term physical security risk mitigation decision making and identify and promote programmatic efficiencies.

   Additionally, Facility Security Assessments are conducted by FPS every three to five years at each General Services Administration (GSA) owned or leased facility in collaboration with USMS, GSA, and the Judiciary Security Division within the Administrative Office of the U.S. Courts. This assessment reviews and identifies security countermeasures that are present, their operating condition, and what may be needed for the facility to achieve appropriate security level status based on the Interagency Security Committee Federal Risk Management Process.

   The Judiciary remains committed to these sound partnerships with the Executive Branch and broader law enforcement community to promote Judiciary security.