Questions for the Record from Representative Darrell Issa for Hon. Michael Scudder
Fiscal Accountability and Oversight of the Federal Courts, Tuesday, 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?

2. Will the Judicial Conference and Administrative Office of the 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?

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?

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?

Questions for the Record from Representative Scott Fitzgerald for Judge 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?