

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

August 25, 2025

The Honorable John G. Roberts, Jr
Chief Justice
Supreme Court of the United States
1 First Street, NE
Washington, DC 20543

Dear Chief Justice Roberts:

The federal judiciary has repeatedly proven itself incapable of protecting the highly sensitive and confidential information with which it has been entrusted. In 2020, the federal judiciary's case management system was reportedly hacked by foreign adversaries. Staggeringly, this year, this same system has been hacked again by foreign actors, reportedly exploiting unresolved vulnerabilities that were discovered five years ago. In light of this most recent hack of the federal judiciary's case management system, I write to request that you commission an independent, public, expert review by the National Academy of Sciences of these two major security incidents, the judiciary's cybersecurity practices, and the judiciary's mismanagement of its own technology.

The federal judiciary's current approach to information technology is a severe threat to our national security. The courts have been entrusted with some of our nation's most confidential and sensitive information, including national security documents that could reveal sources and methods to our adversaries, and sealed criminal charging and investigative documents that could enable suspects to flee from justice or target witnesses. Yet, you continue to refuse to require the federal courts to meet mandatory cybersecurity requirements and allow them to routinely ignore basic cybersecurity best practices. Federal judicial technology and cybersecurity policy is set by a committee of judges whose membership you have kept hidden from the public and who presumably have no technology expertise. The case management system used by the federal courts has been hacked multiple times, in part because the system is insecure, antiquated and expensive to operate. While the judiciary has solicited advice from leading government experts on establishing a modern, secure and efficient case management system, the judiciary thus far has ignored that advice and has made no meaningful progress towards a replacement. These serious problems in the judiciary's approach to cybersecurity have been able to fester for decades because the

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

judiciary covers up its own negligence, has no inspector general and repeatedly stonewalls congressional oversight. This status quo cannot continue.

The judiciary has now repeatedly failed, spectacularly, in its obligation to safeguard the sensitive information it possesses. On August 6, 2025, Politico reported that the federal judiciary's case management system was compromised by hackers, exposing sensitive data entrusted to the courts. The New York Times subsequently reported that "documents related to criminal activity with an overseas tie, across at least eight district courts, were initially believed to have been targeted." This hack should have never happened. According to a follow-up Politico story, the most recent hack "exploited unresolved security holes discovered five years ago." What makes this even more troubling is that this exact same software system was hacked in 2020 by "three hostile foreign actors," according to then-House Judiciary Chairman Jerrold Nadler.

It has now been five years since the 2020 hack and the judiciary has still not revealed what happened. While executive branch agencies and their inspectors general are required to report cybersecurity incidents to Congress and provide substantive briefings about hacks, the judiciary has generally taken the approach of revealing next to nothing and stonewalling congressional oversight. I sent the attached letter to the Director of the Administrative Office of United States Courts (AO) on July 28, 2022, seeking answers to a number of basic questions about the 2020 security breach. The AO refused to answer my oversight questions. There is no legitimate need to keep Congress or the public in the dark about that incident so many years later. I strongly suspect that the judiciary is covering up its own negligence and incompetence which resulted in the security vulnerabilities that the hackers exploited.

The fact that the judiciary is still using this insecure software is a direct result of the judiciary's mismanagement of its own information technology. Judge Michael Scudder, who chairs the Committee on Information Technology of the federal courts' policymaking body, the Judicial Conference, testified before the House Judiciary Committee in June 2025 that the software used for the case management system is "outdated, unsustainable due to cyber risks, and require[s] replacement." This statement is undoubtedly true today and, as the federal judiciary should be well aware, it was true five years ago. Between 2021 and 2022, the AO retained the services of technology experts at the General Services Administration (GSA), who issued three reports describing how the judiciary should build a new case management system at a low cost and with a low risk of the project failing. The experts at GSA recommended that the AO write the software in-house, starting with a single team of 5-7 technologists, who would begin rebuilding the system, one small piece at a time, with regular input from users and demonstrations of new features every few weeks. Had the AO heeded this expert advice in 2022, it is likely that the new case management system would be finished by now. But the AO ignored this advice and then did the exact opposite. Instead, in April 2023 the AO published a lengthy solicitation — containing 188 different requirements

— for government contractors to build a major new search feature for the case management system. Hiring a contractor to build software to a set of complex requirements is exactly the approach the GSA experts advised against. As of December 2024, the AO had still not awarded a contract for this work.

But the judiciary's aging case management software cannot be blamed entirely for these multiple hacks. Plenty of federal agencies use decades-old software. The key difference between the judiciary and these agencies is that executive agencies are subject to minimum federal cybersecurity requirements, while the federal judiciary has not adopted its own set of binding minimum cybersecurity standards that every federal court must follow. Instead, each of the 94 federal district courts and 12 courts of appeals can choose to adopt good or bad practices.

A good example of this difference is in the adoption of multi-factor authentication (MFA), a widely adopted cyberdefense that protects against breaches caused by hackers learning a target's password. Federal agencies have been required by federal law to use MFA since 2015. The Office of Management and Budget raised the bar in 2022, requiring agencies to use the most secure form of MFA, known as phishing-resistant MFA. By contrast, the AO only recently announced that it will finally be requiring MFA for access to the judiciary's case management system by the end of 2025.

Clearly, the judiciary should not have waited five years after three foreign adversaries hacked the case management system to roll out such a basic cyberdefense. But the form of MFA finally adopted by the judiciary is not phishing-resistant, and does not meet federal or industry cybersecurity best practices. The glacial speed with which the federal judiciary adopted this inferior cyberdefense, years after government agencies and businesses have migrated to superior solutions, highlights the fact that the judiciary's cybersecurity problems are not technical, but rather, are the result of incompetence and the total absence of accountability.

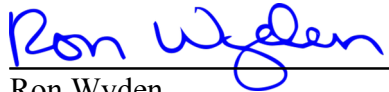
The judiciary's complete failure to address its cybersecurity problems after the 2020 breach, as well as the subsequent coverup and stonewalling of congressional oversight, makes it clear that the judiciary and its policymaking arm, the Judicial Conference, are ill-equipped to diagnose and address their own problems. An independent, public, expert review is essential not only because of repeated hacks, but also because of the judiciary's subsequent lack of transparency. For example, the judiciary still hasn't notified victims whose information was stolen in 2020. Such a review is needed to rebuild the trust of litigators, parties, Congress and the public. Moreover, while I would normally request that the Department of Homeland Security's Cyber Safety Review Board conduct such a review, having the executive branch review the judiciary's cybersecurity could raise separation of powers issues and, regardless,

President Trump fired the whole board on the second day of this administration and has not appointed any new members.

Accordingly, I urge you to commission an independent, public, expert review by the National Academy of Sciences of the 2020 and 2025 hacks of the case management system, the judiciary's cybersecurity practices, and the judiciary's mismanagement of its own technology, including software development and procurement. Please also provide me with a copy of any reports that have been prepared on the 2020 breach, and when a report has been completed on the 2025 breach, please provide a copy of that report too. Finally, I urge you to direct the AO to cooperate with congressional oversight.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

A handwritten signature in blue ink that reads "Ron Wyden". The signature is fluid and cursive, with the first name "Ron" and last name "Wyden" clearly distinguishable. It is positioned above a horizontal line.

Ron Wyden
United States Senator

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

July 28, 2022

The Honorable Roslynn R. Mauskopf
Director
Administrative Office of the U.S. Courts
One Columbus Circle, NE
Washington, DC 20544

Dear Director Mauskopf:

I write to express serious concerns that the federal judiciary has hidden from the American public and many Members of Congress the serious national security consequences of the courts' failure to protect sensitive data to which they have been entrusted.

On the afternoon of January 6, 2021 the federal judiciary issued a press release stating that in December 2020 an investigation by the Department of Homeland Security discovered vulnerabilities in the court records system, CM/ECF, "that greatly risk compromising highly sensitive" sealed court filings. The press release noted that there had been an "apparent compromise" of that system due to an "attack." It has been nearly a year and a half since this cybersecurity breach was discovered. The federal judiciary has yet to publicly explain what happened and has refused multiple requests to provide unclassified briefings to Congress.

The judiciary's flawed court records system, its practice of decentralizing cybersecurity decisions to each court, and its opposition to Congressional efforts to modernize that system, have created unmanageable security risks. Recently, a review of CM/ECF by the General Services Administration found that CM/ECF is "outdated," "obsolete," "not sustainable." Among the report's findings:

- "There is the potential for many cybersecurity vulnerabilities resulting from the way CM/ECF software is built, deployed, and maintained."
- "Security and compliance are monumental tasks for courts and the AO's visibility into courts' security posture is limited due to the decentralized nature of the application."
- "Decentralization and complexity are causing system instability, high maintenance costs and security risks."
- "Dated technology, decentralized deployments, and heavy customization" are causing "security and reliability risks."
- "Many courts have developed 'local mods' ... which has created problems ranging from high cybersecurity risks to high operational costs."

The judiciary has been aware of vulnerabilities in its court records system long before this cybersecurity breach was detected. In 2017, for example, one researcher identified a serious flaw that took the Administrative Office of the Courts (AO) nearly 6 months to fix. As that researcher explained, “the nature and severity of this bug indicates that the AO likely does not have a culture that properly prioritizes security, or that if they do, their current approach to security is not working.”

The cybersecurity problems that plague the CM/ECF system are symptoms of a bigger problem, which is that the federal judiciary is exempt from all mandatory cybersecurity requirements that apply to executive branch agencies, and that it has failed to adopt any similar requirements itself.

Congress has set strict rules for civilian executive branch agencies’ cybersecurity, including minimum cybersecurity standards, and independent audits of agencies’ compliance with those standards. The federal judiciary, by contrast, has no binding minimum security standards. Instead, each of the 94 federal district courts and 12 courts of appeals can choose to adopt good or bad practices, with no central oversight. These courts lack both the resources and expertise to defend against sophisticated foreign hackers.

Forcing the chief judges of individual district and appellate courts, who are not cybersecurity experts, to bear primary responsibility for the judiciary’s cybersecurity was a mistake. The federal judiciary should adopt a set of mandatory cybersecurity standards, similar to those adopted by the executive branch, that all federal courts are required to implement. The AO should also conduct and submit to Congress mandatory audits for compliance.

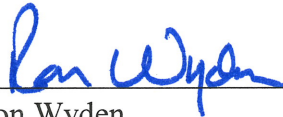
Unfortunately, the federal judiciary has not only opposed the Open Courts Act—bipartisan legislation that would modernize and centralize its vulnerable courts records systems—but specifically opposed a provision in the bill that would ensure that the system meet the same cybersecurity standards that already apply to executive branch agencies. As the General Service Administration report noted, “a headline of a successful cyberattack on CM/ECF will weaken the public’s trust in the judiciary.” But news that the judiciary failed to adequately disclose such an attack and its impact on national security will weaken the public’s trust even more. To that end, I ask that you answer the following questions by August 26, 2022.

1. Had the systems containing the vulnerabilities exploited by the hackers been subjected to cybersecurity audits prior to the breach? If yes, please explain whether these audits discovered the vulnerabilities and they had not been fixed or why the audits failed to identify the vulnerabilities? If no, please explain why these systems were not subjected to audits.
2. When did the hackers first gain unauthorized access to the CM/ECF system? How long did it take for them to be discovered?
3. Did the AO discover the security breach or was it notified by another entity? If the latter, why were the Judiciary’s cyber defenses insufficient to detect the breach?
4. What information was accessed by the hackers?
5. In each of the past 5 years, how many federal courts have taken advantage of the free, voluntary cybersecurity audits offered by the AO? Please provide me with copies of the

results of these audits, any records indicating whether the courts addressed all issues discovered during the audits, and a list of the courts that have not yet requested an audit.

Thank you for your attention to this important issue. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

A handwritten signature in blue ink, appearing to read "Ron Wyden", is written over a horizontal line.

Ron Wyden
United States Senator