

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

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 Recently, a review of CM/ECF by the General Services Administration found that CM/ECF is "outdated," "obsolete," "not sustainable."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."

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

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.

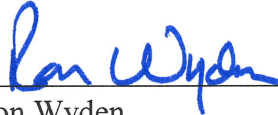
Unfortunately, the federal judiciary has not only opposed the Open Courts Act—bipartisan legislation that would modernize and centralize its vulnerable courts records systems—but specifically opposed a provision in the bill that would ensure that the system meet the same cybersecurity standards that 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,



Ron Wyden
United States Senator