In the United States Court of Federal Claims

(Pro Se)

THEODORE HAUGLAND, Plaintiff, v. THE UNITED STATES OF AMERICA, Defendant.	Case: 1:25-cv-02079-EHM (Filed: January 20, 2026) Judge: Edward H. Meyers

PLAINTIFF'S MOTION FOR PROTECTIVE ORDER

Pursuant to RCFC 5.2(d), RCFC 26(c), and the Court's Inherent Authority

---

I. INTRODUCTION

Plaintiff respectfully moves for entry of a **new Protective Order** governing Plaintiff's sealed filings and confidential information in light of the **August 2025 compromise of the CM/ECF case filing system.**

CM/ECF system was presumed to provide a baseline level of confidentiality consistent with RCFC 5.2(d). That assumption is no longer valid. In August 2025, the Administrative Office of

the U.S. Courts publicly acknowledged that sealed filings within CM/ECF were accessed by unauthorized actors following a system-wide breach.

This constitutes a **material change in circumstances** that warrants renewed and enhanced protective relief. Plaintiff does not seek sanctions or adjudication of responsibility. He seeks prospective measures necessary to ensure that the Court's confidentiality determinations remain meaningful notwithstanding demonstrated system vulnerabilities.

II. History of CM/ECF and PACER Data-Security Breaches

The need for a Protective Order is further supported by the judiciary's documented history of data-security incidents involving CM/ECF and PACER, including the breach disclosed in August 2025 affecting sealed and restricted filings.

A. SolarWinds-Related CM/ECF Compromise (2020–2021)

In December 2020, the Department of Homeland Security issued an emergency directive regarding exploitation of SolarWinds Orion software used across federal systems. The Administrative Office of the U.S. Courts subsequently acknowledged an apparent compromise affecting CM/ECF infrastructure and directed courts to limit electronic filing of highly sensitive materials, including sealed documents, and to utilize paper or secure alternative submission methods.

This incident established that CM/ECF was vulnerable to systemic compromise and that electronic sealing alone did not ensure confidentiality.

B. Federal Judiciary Data-Breach Investigation (2021)

In January 2021, the Department of Justice confirmed that CM/ECF had been accessed during the SolarWinds incident. In March 2021, the House Judiciary Committee reported that the scope of the breach was extensive and that sealed filings may have been exposed.

CM/ECF and PACER nevertheless continued to operate on legacy infrastructure without comprehensive modernization of security controls.

C. Government-Wide Cyber Intrusions (2020)

The CM/ECF compromise occurred contemporaneously with widespread intrusions affecting multiple federal agencies, including the Departments of Treasury, Commerce, and Homeland Security. While executive agencies implemented broad cybersecurity reforms, the judiciary remained dependent on legacy systems with limited external oversight.

D. Continued Vulnerabilities and Limited Oversight

Subsequent analyses continued to identify risks associated with CM/ECF. In 2021, legal and cybersecurity commentators described the system as presenting ongoing data-security concerns for litigants. In 2023, presentations before the FOIA Advisory Committee highlighted the judiciary's exemption from FOIA and the resulting lack of public visibility into information-technology failures or remediation efforts.

E. August 2025 CM/ECF and PACER Breach Affecting Sealed Filings

In August 2025, the federal judiciary publicly disclosed a data-security incident involving CM/ECF and PACER that raised concerns regarding unauthorized access to sealed and restricted filings. Guidance issued following the incident advised courts and litigants to limit electronic submission of particularly sensitive materials and to review filing practices for protected information.

Judicial Conference testimony in 2025 further acknowledged that CM/ECF was outdated, subject to recurring cyber risks, and that sealed records—including indictments and warrants—had been targeted.

III. LEGAL AUTHORITY

A. RCFC 5.2(d)

RCFC 5.2(d) authorizes the Court to seal filings and to control access to them. Where circumstances change such that existing protections are no longer sufficient, the Court retains continuing authority to impose additional or modified safeguards to preserve confidentiality.

A sealing order necessarily carries with it the authority to ensure that sealing remains effective.

B. RCFC 26(c)

RCFC 26(c) authorizes the Court, for good cause, to issue protective orders to prevent disclosure, limit access, and prescribe conditions for handling sensitive materials. Courts routinely rely on Rule 26(c) to impose protective measures outside the discovery context when confidential judicial records are at risk.

Good cause exists where a demonstrated security breach creates an ongoing risk of further disclosure.

C. Inherent Authority of the Court

This Court possesses inherent authority to manage its docket, protect litigants, and ensure compliance with its orders. *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 36 (1984). That authority includes issuing new or supplemental protective orders when prior assumptions regarding confidentiality no longer hold.

IV. GOOD CAUSE FOR A NEW PROTECTIVE ORDER

The August 2025 CM/ECF breach constitutes good cause for entry of a new protective order for several reasons:

- The Court has already determined that Plaintiff's filings warrant sealing;
- The integrity of the electronic system relied upon to enforce that sealing has been compromised;
- The risk of secondary dissemination or misuse of sealed information remains ongoing; and
- Absent additional safeguards, the Court's prior confidentiality determination cannot be reliably enforced.

Once confidential judicial material is disclosed, the harm cannot be undone. Preventative, forward-looking relief is therefore necessary to mitigate continuing risk.

V. REQUESTED PROTECTIVE RELIEF

Plaintiff respectfully requests that the Court enter a **new Protective Order** providing that:

1. **Plaintiff's sealed complaint and any materials derived therefrom shall not be accessed, disclosed, copied, or used** except by express authorization of the Court;

2. **Defendant shall certify in writing** the measures currently in place to restrict access to Plaintiff's sealed filings in light of the CM/ECF breach;

3. **Any copies or extracts** of Plaintiff's sealed materials obtained through unauthorized access shall be segregated and not further disseminated;

4. **Plaintiff's sealed materials shall not be used** in this or any other proceeding, administrative or judicial, absent prior Court approval;

5. **Access to Plaintiff's sealed filings shall be limited** to the Court and individuals expressly authorized by Court order; and

6. The Court may impose **such additional protective measures** as it deems necessary to ensure that its confidentiality determinations remain effective notwithstanding system vulnerabilities.

These measures are narrowly tailored, prospective, and directly responsive to the changed circumstances created by the August 2025 breach.

VI. CONCLUSION

Entry of a new Protective Order is necessary to preserve the effectiveness of the Court's confidentiality determinations and to prevent further prejudice resulting from demonstrated system vulnerabilities.

Respectfully Submitted,

January 20, 2026
Date

/s/ Theodore Haugland
THEODORE HAUGLAND
Plaintiff, *Pro Se*
99-009 Kalaloa St
Unit D2016
Aiea, HI 96701
United States
(202)933-3332
theodorehaugland@outlook.com
Case: 1:25-CV-02079-EHM

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.

Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System

Published on August 7, 2025

The federal Judiciary is taking additional steps to strengthen protections for sensitive case documents in response to recent escalated cyberattacks of a sophisticated and persistent nature on its case management system. The Judiciary is also further enhancing security of the system and to block future attacks, and it is prioritizing working with courts to mitigate the impact on litigants.

The Administrative Office of the United States Courts has continued to collaborate with Congress as well as the Department of Justice, the Department of Homeland Security and other partners in the executive branch to mitigate the risks and impacts of these cyberattacks.

The vast majority of documents filed with the Judiciary's electronic case management system are not confidential and indeed are readily available to the public, which is fundamental to an open and transparent judicial system. However, some filings contain confidential or proprietary information that are sealed from public view.

These sensitive documents can be targets of interest to a range of threat actors. To better protect them, courts have been implementing more rigorous procedures to restrict access to sensitive documents under carefully controlled and monitored circumstances.

Enhancing the security of its systems is a top priority for the Judiciary. Over the past few years, the Judiciary has added significant cybersecurity protections and safeguards to the case management system. The Chairman of the Judicial Conference's Committee on Information Technology, Court of Appeals Judge Michael Y. Scudder, briefed the Conference and the media in September 2024 on potential threats to Judiciary IT systems and steps taken by the Judiciary to address them. Subsequently, in June of this year Judge Scudder testified before a House Judiciary subcommittee and underscored the Judiciary's ongoing commitment to investing in and modernizing its IT systems in order to confront the constant and increasingly sophisticated cybersecurity threats the branch faces.

As other federal government and private entities likewise continue to experience, cyber risks continue to evolve as threat actors grow more sophisticated and change and adapt their tactics, and safeguarding legacy systems poses a particularly difficult challenge. In tackling cybersecurity threats, the Judiciary embraces its security obligations and remains committed to leveraging all available resources to include collaboration with law enforcement, national security and cybersecurity organizations, and other information sharing entities.

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

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,

Ron Wyden
United States Senator

Judiciary Restricts Access to Sealed Records After Cyber Hack

Sept. 24, 2025, 12:04 PM PDT

Federal trial courts are issuing new orders restricting access to sealed documents, following a directive from the judiciary's administrative office to address escalated cyberattacks targeting the courts' case system.

The standing orders, posted by more than 20 federal courts across the US since Monday, state that while sealed documents may be filed within the judiciary's online case management system, known as CM/ECF, those documents won't be able to be viewed or accessed electronically.

The orders are intended to comply with recent instructions by the Administrative Office of the US Courts to federal courts to further restrict sealed documents, multiple federal court notices said.

The judiciary's administrative office is implementing a new Sealed Document Security system, which was scheduled to take effect Tuesday pending successful testing, "to address identified security vulnerabilities and strengthen the protection of restricted filings," according to a notice posted by the New Mexico federal trial court.

A spokesperson for the AO said the judiciary is "continuously working in collaboration with Congress and our law enforcement partners to strengthen protections for sensitive case documents," and declined to comment further on the changes.

The changes come over a month after the judiciary revealed it had experienced "escalated cyberattacks of a sophisticated and persistent nature" on its case management system. The management system includes Case Management/Electronic Case Files (CM/ECF), used to upload court papers, and PACER, which allows the public to access some court documents.

The hackers targeted sealed documents in espionage and other sensitive cases in a breach of the case management system, using similar vulnerabilities exploited in another hack five years ago, Bloomberg Law has reported. Bloomberg News reported that Russian government hackers lurked for years in the judiciary's records system.

A classified briefing was held on Sept. 9 in the Senate about the cyber attack against the judiciary, according to Josh Sorbe, a spokesperson for Sen. Dick Durbin (D-Ill), the top Democrat on the Judiciary Committee. Lawmakers on committees handling issues affecting the judiciary, funding for the courts, and intelligence were seen entering the meeting.

In some cases, the judiciary's new guidance would loosen restrictions put in place this summer in response to the latest breach on the judiciary's system.

The US District Court for the Eastern District of Virginia, known for handling high-profile national security cases, issued an order in late July requiring that all sealed documents be filed as hard copies only.

The federal trial court in Maryland issued an order in August changing its filing procedures for sealed documents in criminal cases, and the new guidance means those documents "may once again be filed electronically," according to a standing order posted Wednesday by the court.

To contact the reporter on this story: Suzanne Monyak at smonyak@bloombergindustry.com

To contact the editors responsible for this story: Seth Stern at sstern@bloomberglaw.com; John Crawley at jcrawley@bloomberglaw.com

MAYER|BROWN

NOVEMBER 21, 2025

'MORE RULES AND HURDLES': US CHIEF JUDGES ADOPT CYBERSECURITY SEALED DOCUMENT SAFEGUARDS

RELATED PEOPLE:
ADAM S. HICKEY

GENERATE PDF

To read complete article visit The National Law Journal

SHARE

U.S. chief district judges in multiple jurisdictions, including the Southern District of New York and Eastern District of Virginia, now require parties to serve opposing counsel with sealed documents outside of the federal judiciary's electronic filing system following recent cyberattacks on the judiciary's virtual assets.

Federal trial courts are increasingly governed by standing orders restricting online access to sealed documents, effectively requiring high-stakes litigators to serve opposing parties with sealed documents through consensual private arrangements or nonelectronic means.

The new cybersecurity safeguards can make litigation matters more costly, less efficient and even invite new risks of their own, according to business litigators.

Unauthorized users launched a series of 2025 cyberattacks on the federal Case Management/Electronic Case Files system. The identities of the hackers have not been publicly identified, but a New York Times story suggests the hacking could possibly have been perpetrated by Russian state-linked actors.

"Because sealed documents filed in CM/ECF will not be accessible or viewable by litigants electronically, service of those documents can no longer be accomplished through CM/ECF," U.S. Chief District Judge Mark S. Davis of the Eastern District of Virginia wrote in a standing order filed in September.

"After filing sealed documents on CM/ECF, parties will have to serve the sealed documents by other appropriate means as provided by the Federal Rules of Procedure," Davis added, citing Federal Rule of Civil Procedure 5.

Sealed documents in civil litigation may include proprietary or trade secret information of the parties, confidential personal information, financial records or executive communications, among other sensitive data, according to Monte Mann, a business litigation partner at Armstrong Teasdale.

The requirement for parties to serve sealed documents under Rule 5 prioritizes security over convenience but introduces the risk of gamesmanship between opposing counsel, Mann said in an interview.

"When there are more rules and hurdles on the parties, there can be disputes among the parties over those rules," he added. "Parties may serve each other with unredacted copies of sealed documents under Rule 5, which may include electronically by email if the parties consent to service that way."

"The practical effect—it is going to make business litigators' life a little harder," Mann said. "It's going to make us take extra steps."

One risk with the new standing orders in jurisdictions like the Southern District of Illinois and elsewhere is that parties could "weaponize [Rule 5] to their advantage" by claiming opposing counsel delayed service of sealed documents, Mann said. "In a perfect world, I hope it doesn't, [but] it may."

David Gringer, an antitrust litigation partner at Wilmer Cutler Pickering Hale and Dorr, said the

federal judiciary has done a "pretty good job" minimizing cybersecurity breaches.

"There needs to be a recognition that courts are holding sensitive information," Gringer told law.com and the National Law Journal. "Once something leaves where you are and goes someplace else, there are risks. Those risks cannot be eliminated; they can only be mitigated."

Clients are "increasingly worried" about the risk of cyberattacks, Gringer added. "It is a really scary world out there, and there is no such thing as a guarantee of security for sensitive or nonsensitive information, and there's a lot of bad actors out there."

The federal judiciary in 2021 began restricting electronic access to highly sensitive documents or HSDs following the December 2020 cyberattacks on SolarWinds, a tool for managing data networks.

"In many ways, this is not really new," Matthew Wright, a managing partner at the McCarter & English D.C. office, said of the new protocols surrounding sealed documents. "There have always been constraints and restrictions around the handling of sensitive materials."

The "best practice" to prevent sealed documents from landing in the wrong hands is to transfer physical documents to parties "in person with someone who shows ID and proves they are associated with counsel of record," said cybersecurity and data privacy expert Adam S. Hickey.

"Once you are relying on remote communication like email, telephone or video chat there is a potential for mischief," added Hickey, a partner at Mayer Brown. "Even the best practices won't be foolproof."

In the United States Court of Federal Claims

THEODORE HAUGLAND
Plaintiff(s),

v.

THE UNITED STATES,

Defendant.

Case No. 1:25-cv-02079-EHM

Judge Edward H. Meyers

CERTIFICATE OF SERVICE

I hereby certify that on January 20, 2026, a copy of plaintiffs motion for protective order, was mailed via USPS Certified Mail, to Eric J. Smith, at PO Box 26, Washington, DC 20530.

Theodore Haugland
(Signature of Applicant)

Theodore Haugland
(Printed Name)

99-009 Kalaloa St # D2016
(Street Address)

Aiea, HI 96701
(City, State, ZIP Code)

(202)933-3332
(Phone Number)

UNITED STATES POSTAL SERVICE®

LEGAL

C

RETURN SERVICE REQUESTED

CERTIFIED LEGAL MAIL

THEODORE HAUGLAND
99-009 KALALOA ST
UNIT D2016
AIEA, HI 96701

CERTIFIED

UNITED STATES COURT OF FEDERAL CLAIMS
ATTENTION: COURT CLERK
717 MADISON PLACE, NW
WASHINTON, DC 20439-0001

F

US POSTAGE IMI 059260120041513 2000394174
$8.58
SSK
FCM

01/20/26 Mailed from 96820 028W2311536

USPS FIRST-CLASS MAIL®

THEODORE HAUGLAND
APT D2016
99-009 KALALOA ST
AIEA HI 96701-3498

RECEIVED
JAN 30 2026
OFFICE OF THE CLERK
U.S. COURT OF FEDERAL CLAIMS

6.52 oz
RDC 99

SHIP TO:
USCFC
Attn: Court Clerk
~~ERIC S SMITH~~ 717 Madison PL, NW
WASHINGTON DC 20439

USPS CERTIFIED MAIL®

9507 1067 1411 6020 3888 47