



# JUDICIAL CONFERENCE OF THE UNITED STATES

WASHINGTON, D.C. 20544

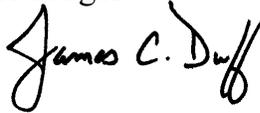
THE CHIEF JUSTICE  
OF THE UNITED STATES  
*Presiding*

JAMES C. DUFF  
*Secretary*

January 6, 2021

## MEMORANDUM

To: All United States Judges

From: James C. Duff 

RE: POLICY CHANGE FOR SEALED FILINGS IN CM/ECF  
**(URGENT ACTION REQUIRED)**

Recent news reports revealed significant cybersecurity breaches into the computer systems of federal agencies. These reports indicate that the breaches possibly were caused by nation state actors as part of a global espionage campaign with confirmed instances of compromise of highly sensitive information in those systems. The Administrative Office of the U.S. Courts (AO) is working with the Department of Homeland Security on a security audit of our most sensitive and critical computer application, the Case Management/Electronic Case Filing (CM/ECF) system. This action is endorsed by the Judicial Conference's Executive Committee and supported by the Conference's Information Technology and Court Administration and Case Management Committees. That audit indicates serious security vulnerabilities in CM/ECF that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings. An apparent compromise of the confidentiality of the CM/ECF system due to these discovered vulnerabilities currently is under investigation.

The Federal Judiciary has long applied a strong presumption in favor of public access to documents. Court rules and orders should presume that every document filed in or by a court will be in the public domain, unless the court orders it to be sealed, and that documents should be sealed only when necessary. Certain sealed filings in CM/ECF, however, contain sensitive non-public information that, if obtained without authorization and improperly released, could cause harm to the United States, the Federal Judiciary, litigants, and others.

**Your immediate action is needed to mitigate this apparent compromise and reduce the risk of future compromises of confidential court filings.** The Executive Committee considers it imperative that all courts make it a high priority to take the following steps to protect the security of certain highly confidential sealed filings

maintained in their court's electronic files in CM/ECF. The AO will provide guidance for implementing these new procedures, with input from the relevant advisory groups.

### **URGENT ACTION REQUIRED**

- To the extent they have not already done so, all courts should issue a standing or general order or adopt some other equivalent procedure requiring that highly sensitive documents (HSDs) will be accepted for filing only in paper form or via a secure electronic device. HSDs should be stored in a secure paper filing system or a secure standalone computer system that is not connected to any network, particularly the internet. The AO will provide courts with model language for a standing or general order as well as advice and guidance on how to establish and securely maintain a standalone computer system if a court chooses that option.
- This change in procedure should apply to all HSDs filed with the court. However, not every currently sealed filing should be considered an HSD; courts should use their discretion in determining which documents require HSD protection and thus should not reside on CM/ECF and which may continue to be entered into CM/ECF using that court's current sealing practices. Pleadings such as Title III applications and search warrants initially should be considered HSDs. Courts are cautioned not to be overinclusive in determining what is an HSD, as many pleadings currently filed under seal in CM/ECF do not merit the heightened protections addressed in this notice. For example, most documents similar to and including presentence reports, pretrial release reports, pleadings related to cooperation in most criminal cases, social security records, administrative immigration records, and sealed filings in many civil cases likely would not be sufficiently sensitive to require HSD treatment and could continue to be sealed in CM/ECF as necessary. Each court's standing or general order or equivalent procedure should address the types of filings it does and does not consider to be HSDs.
- Accompanying public docket entries for HSDs should not include personal or other identifying details related to those HSDs.
- Sealed court orders and any other sealed documents generated by the court pertaining to HSDs should not be uploaded into CM/ECF or the Public Access to Court Electronic Records (PACER) system or into any other system connected to a network or the internet, but must instead be transmitted to parties by a secure means specified by the court. The AO will provide further guidance regarding such transmissions.
- With respect to filings pertaining to highly sensitive information previously filed in CM/ECF, litigants may request that such sealed cases, matters, or filings be

removed from CM/ECF expeditiously. The manner in which parties may make such a request should be included in your standing or general order. The court should file and retain materials that are removed from CM/ECF in a secure paper filing system or standalone computer as described above.

The Executive Committee fully appreciates the practical implications of taking these steps and the administrative burden this will place on courts. Yet, it has determined that any such burdens are outweighed by the need to preserve the confidentiality of sealed filings that are at risk of compromise. The Federal Judiciary's foremost concern must be the integrity of and public trust in the operation and the administration of its courts.

cc: Circuit Executives  
District Court Executives  
Clerks, United States Courts