IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

IN RE: PROCEDURES FOR THE FILING, SERVICE, AND MANAGEMENT OF HIGHLY SENSITIVE DOCUMENTS	)))))	GENERAL ORDER

WHEREAS, in response to recent disclosures of wide-spread breaches of both private sector and government computer systems, federal courts are immediately adding new security procedures to protect highly sensitive documents (HSDs) filed with the courts;

THE COURT FINDS that, pursuant to Civil Rule 5(d)(3)(A) and Criminal Rule 49(b)(3)(A), good cause exists to (1) require all parties to file certain highly sensitive documents, ("HSDs") outside of the court's electronic filing system and (2) adopt the revised HSD Guidance (Attachment A), which includes a standard definition of HSDs, a dedicated procedure for filing, serving, and maintaining HSDs, and factors to be considered by judicial officers in determining if a document is an HSD.

THERERFORE, IT IS HEREBY ORDERED that, effective as of the date of this order and until such time as the court orders otherwise, the filing of certain HSDs shall be subject to the procedures and requirements set forth below. This General Order supersedes any and all inconsistent provisions in existing local rules or other general orders of this court.

1. **Documents Subject to this Order**

HSDs are defined in terms of (a) subject matter and (b) type of document.

a. In terms of subject matter, HSDs are documents potentially related to or affecting the United States' international interests and consist primarily of documents that may impair the United States' interests if revealed to a foreign power or its agents (as defined by 50 U.S.C. § 1801), would assist a foreign power or its agents in the development of that foreign power's competing commercial products or products with military applications, or potentially negatively impact the reputational interest of the United States.

b. The following types of documents satisfying the description in 1.a above qualify as HSDs: Applications for search warrants, applications for electronic surveillance under 18 U.S.C. § 2518, applications for pen registers and trap and trace devices

under 18 U.S.C. § 3123, and any other document, by order of a judge on the judge's own motion, or by order of a judge upon motion of any party in any matter.

c. Any dispute as to whether a document is an HSD shall be resolved by the presiding judge or, when no presiding judge is assigned, the chief judge.

2. Filing of HSDs

a. When requesting the court designate documents as HSDs, a party must submit to the clerk's office a motion requesting designation of documents as HSDs, setting forth the reasons why the documents should be considered as HSDs under the criteria set out in paragraph 1 of this order and attach the proposed HSDs to the motion. The motion must state the identity of any persons who are to have access to the documents without further order of the Court. The motion and proposed HSDs should be provided in the form of one paper copy and one electronic copy on a secure electronic device such as a password protected thumb drive.

b. A party filing an HSD pursuant to a court order or applicable law shall submit to the clerk's office the HSD, the certificate of service, and a copy of the court order authorizing the treatment of that document as highly sensitive in the form of one paper copy and an electronic copy on a secure electronic device such as a password protected thumb drive.

c. The required documents and the secure electronic device shall be submitted to the clerk's office in a sealed envelope marked "HIGHLY SENSITIVE DOCUMENT." The outside of the envelope shall be affixed with a copy of the HSD's caption page (with confidential information redacted).

d. The filing party shall serve the HSD on the other parties as follows:
   i. Civil cases - by any manner specified in Civil Rule 5(b)(2), except for service via the court's electronic filing system; or
   ii. Criminal cases - by any manner specified in Criminal Rule 49(a)(3)(B) or (a)(4).

3. Highly Sensitive Court Orders

If the court determines that a court order contains highly sensitive information, the clerk's office will file and maintain the order in a secure paper filing system or a secure standalone computer system that is not connected to any network and will serve paper copies of the order on the parties via mail.

4. Removal of Existing HSDs or Highly Sensitive Cases from the Court's Electronic Filing System

Upon motion of a party or upon its own motion, the court may determine that a document, case, or any portion of it, that has been filed electronically is highly sensitive and direct that the HSD or case be removed from the court's electronic filing system and maintained by the clerk's office in a secure paper filing system or a secure standalone computer system that is not connected to any network.

IT IS SO ORDERED, this 25th day of July, 2024.

/s/ Beth Phillips
Beth Phillips
Chief United States District Judge
Western District of Missouri

HIGHLY SENSITIVE DOCUMENTS DEFINITION & GUIDANCE

Highly Sensitive Documents (HSDs) are a narrow subset of sealed documents that must, for their protection, be stored offline. The added protection for HSDs is important because, in the event of a breach of the courts' electronic case management system by a sophisticated actor, those documents are more likely to be sought out and stolen, or their unauthorized access or exposure are likely to have outsized consequences beyond that of most sealed documents, or both.

The following definition and guidance are intended to assist courts in identifying highly sensitive documents and managing the offline handling of HSDs. This guidance does not apply to classified information, which should be handled according to the Classified Information Procedures Act (CIPA) and the Chief Justice's Security Procedures related thereto, 18 U.S.C. app 3 §§ 1, 9(a).[1]

(a) **Definition:** A **Highly Sensitive Document (HSD)** is a document or other material that contains sensitive, but unclassified, information that warrants exceptional handling and storage procedures to prevent significant consequences that could result if such information were obtained or disclosed in an unauthorized way. Although frequently related to law enforcement materials, especially sensitive information in a civil case could also qualify for HSD treatment.

i. **Examples of HSDs:** Examples include *ex parte* sealed filings relating to: national security investigations, cyber investigations, and especially sensitive public corruption investigations; and documents containing a highly exploitable trade secret, financial information, or computer source code belonging to a private entity, the disclosure of which could have significant national or international repercussions.

ii. **Exclusions:** Most materials currently filed under seal do not meet the definition of an HSD and do not merit the heightened protections afforded to HSDs. The form or nature of the document, by itself,

---

[1] The Chief Justice's Security Procedures (criminal prosecutions) and the Department of Justice (DOJ) regulation 28 C.F.R. § 17.17(c) (civil actions) govern classified information in any form in the custody of a court. Such classified information may not be filed on CM/ECF or any other court network or standalone computer system. Courts are assisted in their protection of classified information by classified information security officers, who are detailed to the courts by the DOJ's Litigation Security Group, a unit independent of the attorneys representing the government. Courts should direct questions regarding how to handle classified documents to the DOJ's Litigation Security Group. See also, Robert Timothy Reagan, Keeping Government Secrets: A Pocket Guide on the State-Secrets Privilege, the Classified Information Procedures Act and Classified Information Security Officers, (Federal Judicial Center, 2d ed. 2013).

does not determine whether HSD treatment is warranted. Instead, the focus is on the severity of the consequences for the parties or the public should the document be accessed without authorization. Most presentence reports, pretrial release reports, pleadings related to cooperation in criminal cases, social security records, administrative immigration records, applications for search warrants, interception of wire, oral, or electronic communications under 18 U.S.C. § 2518, and applications for pen registers, trap, and trace devices would not meet the HSD definition.

(b) **HSDs: Sources and Characteristics**

i. HSD designation may be requested by a party in a criminal, civil, appellate, or bankruptcy matter.

ii. HSDs vary in their physical form and characteristics. They may be paper, electronic, audiovisual, microform, or other media. The term "document" includes all recorded information, regardless of its physical form or characteristics.

iii. An opinion or order entered by the court related to an HSD may itself constitute an HSD, if it reveals sensitive information in the HSD.

iv. An HSD in the lower court's record will ordinarily be also regarded by an appellate court as an HSD.

(c) **HSD Designation:**

i. A court's standing order, general order, or equivalent directive should include the HSD definition set forth in (a) above and outline procedures for requesting, filing, and maintaining HSDs.

ii. The onus is on the party, including the Department of Justice and other law enforcement agencies, to identify for the court those documents that the party believes qualify as HSDs and the basis for that belief. In moving for HSD treatment, the filing party must articulate why HSD treatment is warranted, including, as appropriate: the contents of the document; the nature of the investigation or litigation; and the potential consequences to the parties, the public, or national interests, in the event the information contained in the document is accessed or disseminated without authorization.

iii. **Judicial Determination:**

A. The presiding judge (or, when no presiding judge is available, the chief judge) should determine whether a document meets the HSD definition by evaluating whether a party has properly articulated sufficient reasons for such treatment, including the consequences for the matter, should the document be exposed. Most applications for HSD treatment are likely to be *ex parte*, but the presiding judge should resolve any disputes about whether a document qualifies as an HSD as defined in (a) above. The fact that a document may contain sensitive, proprietary, confidential, personally identifying, or financial information about an entity or an individual, that may justify sealing of the document or case, does not alone qualify the document as an HSD.

B. In making this determination, the court should consider properly articulated concerns that the unauthorized access or disclosure of the information contained in the document at issue would result in significant adverse consequences that outweigh the administrative burden of handling the document as an HSD. As a general matter, courts should give careful and appropriate consideration to the concerns articulated by the executive branch in matters implicating the authority of the executive branch to oversee the military and safeguard national security. If relevant, the court has the discretion to consider the impact of the heightened protection provided by offline placement to any other party's right of access.

(d) **Exceptional Administrative Treatment for HSDs:**

i. **Filing:** HSDs and requests for HSD treatment will be accepted for filing only in paper form or via a secure electronic device (*e.g.*, USB stick or portable hard drive).

ii. **Handling:** The court must handle the HSDs by storing all information offline. Furthermore, any pleadings or other filings created in connection with the proceedings should not disclose the subject matter of the HSD (including information that may identify the place, object, or subject of an *ex parte* filing).

iii. **Docketing:** Docket entries for HSDs should not include personal or other identifying details related to or contained within them. For example:

8/25/22 [no link] SYSTEM ENTRY-Docket Entry 92
Restricted until further notice (Entered 8/25/22).

iv. **Storing:** HSDs shall be stored and handled only in a secure paper filing system, or an encrypted external hard drive attached to an air-gapped system (*i.e.*, entirely disconnected from networks and systems, including a court unit's local area network and the judiciary's network).

v. **Safeguarding Internal Communication:** Care should also be taken in judicial communications regarding HSDs, including notes and pre-decisional materials, not to include the protected substance of HSDs in any communication using the internet or a computer network.

(e) **Duration of HSD Treatment:** HSDs are stored temporarily or permanently offline as the situation requires. When designating a document as an HSD, courts should indicate when the designation will automatically lapse or when the designation should be revisited by the judicial officer. HSDs should be migrated as sealed documents to the court's electronic docketing system and unsealed, as appropriate, as soon as the situation allows.