UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF LOUISIANA

IN RE:	GENERAL ORDER
UPDATED PROCEDURES FOR THE FILING, SERVICE, AND MANAGEMENT OF HIGHLY SENSITIVE DOCUMENTS	NO. 2024-12

WHEREAS federal courts are updating their security procedures to uniformly protect highly sensitive documents ("HSDs"), a narrow subset of sealed documents that must, for their protection, be stored outside the court's electronic systems;

THE COURT FINDS that, good cause exists to permit nonelectronic filing under Civil Rule 5(d)(3)(A) and Criminal Rule 49(b)(3)(A), and to adopt the revised HSD guidance, provided herewith as 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.

THEREFORE, 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 highly sensitive documents, as defined herein, shall be subject to the procedures and requirements set forth below. This General Order supersedes any and all inconsistent provisions in existing local rules, administrative procedures, or other general orders of this court. It is presumed that documents filed under seal through the court's current electronic filing system remain secure, and any party moving to file documents under this General Order bear the burden to justify such exceptional treatment. This General

Order does not limit or preclude the filing of documents under seal (containing proprietary or confidential information) in accordance with existing procedures.

1. **Documents Subject to this Order**

   The filing procedures set forth below apply to documents that contain highly sensitive information ("HSI"). Documents containing HSI shall be known as Highly Sensitive Documents ("HSDs"). An 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. 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.

   a. HSI does not refer to all sensitive or confidential information. Instead, HSDs refer only to documents containing information that is likely to be of interest to the intelligence service of a foreign government and whose use or disclosure by a hostile foreign government would likely cause significant harm to the United States or its interests. HSDs 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.

b. 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, 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. Applications for search warrants and applications for interception of wire, oral or electronic communications under 18 U.S.C. § 2518, including but not limited to applications for pen registers, trap and trace devices, and wiretaps, may contain HSI but are not presumptively HSDs. If the filer considers an application under this section 1.b. to contain HSI, the filer shall file a motion to designate the document as an HSD as provided in section 2 below.

c. HSDs do not include pretrial release reports, presentence reports or related documents, pleadings related to cooperation in criminal cases, social security administrative records, immigration administrative records, and most sealed documents in civil cases. Unless the documents identified in this section 1.c. are considered by the filer to contain HSI, they shall continue to be filed under existing sealing procedures.

d. 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. A

judge may decide *sua sponte* to treat any document as an HSD, whether or not a party has sought such designation.

e. If a document cannot be designated as an HSD, a party retains the ability to file such a document in the court's CM/ECF system under seal in accordance with local rules and administrative procedures.

2. Filing of Motions to Treat a Document as an HSD

a. Any filer seeking to have a document treated as an HSD shall file a sealed motion to designate a document as an HSD and proposed order in accordance with the Middle District's Administrative Procedures for Filing Electronic Documents, Section II, except that the proposed HSD shall not be filed electronically. The proposed HSD shall be filed in accordance with the procedures set forth in section 4.

b. The motion to designate the document as an HSD shall set forth why the proposed document constitutes an HSD under the criteria set forth in section 1.a. and 1.b. or why it should otherwise be subject to the heightened protection for HSDs, including, as appropriate: a summary of 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. The motion shall not disclose any information that divulges any HSI. The motion must also be accompanied by a certification of the movant's good-faith belief that the material meets the HSD definition.

c. The court will issue an order on the motion and, if granted, an informational entry will be made on the case docket indicating that the HSD has been filed with the court. The order will identify the persons who are to have access to the documents without further order of the court and will set forth instructions for the duration of HSD treatment or if the designation shall be revisited by the judicial officer within a certain period of time. The clerk's office will maintain the HSD in a secure paper filing system or a secure standalone computer system that is not connected to any network.

3. Service of 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. Procedures for Conventionally Filing an HSD

a. Within 3 business days of filing the motion to designate a document as an HSD, the filing party shall deliver to the clerk's office (in-person or via U.S. Mail) the proposed HSD and certificate of service (if required by statute or rule), plus two copies. If the proposed HSD is voluminous (over 20 megabytes), the filing party may motion the court for permission to submit the proposed HSD to the clerk's office via secure alternative media deemed acceptable by the clerk's office.

b. The upper right portion of the document's case caption shall include the designation of "SEALED" and "HSD".

c. If submitted in person, the required documents, unfolded, 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). In the case of a voluminous exhibit submitted to the clerk's office after receiving leave of court as set forth in section 4.a., the media itself must be labeled and then placed inside a sealed opaque envelope marked "HIGHLY SENSITIVE DOCUMENT."

d. If submitted by U.S. mail, the required documents shall be packaged as set forth in section 4.c., except that the package must be placed in an additional sealed opaque envelope that does not provide any indication of the envelope's contents.

e. If a statute or rule requires service of a motion filed under section 2.a. on opposing parties, the proposed HSD shall be served, 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).

f. The clerk's office will make an informational docket entry in the court's electronic filing system indicating that the HSD was filed with the court and

will maintain the HSD in a secure paper filing system or a secure standalone computer system that is not connected to any network.

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

a. Upon the filing of a motion to remove HSD or HSI by a party (in accordance with the procedures set forth in section 2.a.) 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.

b. A party's sealed motion to remove a HSD or a highly sensitive case from the court's electronic filing system shall identify the specific document number to be designated as a HSD and set forth why such document or case is highly sensitive under the criteria set out in section 1.a. or 1.b. or why it should otherwise be subject to the heightened protection for HSDs. The motion shall not disclose any information that divulges any HSI.

6. Safeguarding Internal Communication

The court will take care in internal court 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 connected to a network.

7. **Questions about HSD Filing Procedures**

Any questions about how an HSD should be filed with the court pursuant to this General Order should be directed to the clerk's office at (225) 389-3500.

IT IS SO ORDERED, this 29th day of July 2024.

Shelly D. Dick

SHELLY D. DICK
CHIEF UNITED STATES JUDGE
MIDDLE DISTRICT OF LOUISIANA

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).

Attachment A

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.