


APR 30 2024

By: 
Deputy Clerk

UNITED STATES BANKRUPTCY COURT
NORTHERN DISTRICT OF GEORGIA

IN RE: PROCEDURES FOR REQUESTING, : AMENDED AND RESTATED
FILING, AND MANAGEMENT OF : GENERAL ORDER 44-2021
HIGHLY SENSITIVE DOCUMENTS :

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, pursuant to Fed. R. Civ. P. 5(d)(3)(A) and Fed. R. Bankr. P. 5005(a)(2)(A) and 7005(d)(3)(A), good cause exists to permit nonelectronic filing and to 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.

THEREFORE, IT IS HEREBY ORDERED that, effective as of the date of this order and until such time as the court orders otherwise, HSDs will be filed and served in paper form (or, if digital media, on a secure electronic device), in accordance with this Order and the HSD Guidance, and will be maintained by the clerk's office in a secure paper filing system or secure standalone computer system that is not connected to any network. This Order supersedes General Order 44-2021 entered January 14, 2021 and any inconsistent local rules concerning HSDs.

1. Documents and Materials Subject to this Order

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 manner. 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, 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 bank records, personally identifiable information, social security records, health records, sealed qui tam cases, and sealed filings in most bankruptcy cases and adversary proceedings would not meet the HSD definition. Notwithstanding the foregoing, the Court retains the authority to seal documents that are not HSDs pursuant to 11 U.S.C. Section 107.

- b. 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.

2. Requesting HSD Designation

A party seeking to file an HSD first must obtain an order authorizing the treatment of the filing as an HSD by filing a motion using these procedures.

a. Represented Parties

- i. A represented party must electronically file a motion to treat a document as an HSD together with a proposed order as provided for in Local Rule 5005-5 and 5005-6 (b)(5), except that the proposed HSD itself must not be filed electronically. The motion must be accompanied by a certification of the movant’s good-faith belief that the material meets the HSD definition set out in paragraph 1 above. The requesting 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.
- ii. As soon as practicable after the motion is filed, the filing party must deliver to the clerk’s office two paper copies of: the HSD sought to be filed and a certificate of service demonstrating compliance with paragraph 2.c. The required documents, unfolded, must be submitted to the clerk’s

office in a sealed envelope marked “HIGHLY SENSITIVE DOCUMENT.” The outside of the envelope must be affixed with a copy of the HSD’s caption page (with confidential information redacted) and with a copy of the notice of electronic filing generated from CM/ECF upon the filing of the motion to treat the document as highly sensitive.

b. Pro Se Parties

Pro se parties must submit to the clerk’s office for filing two paper copies of: a motion to treat a document as an HSD, the HSD sought to be filed, and a certificate of service demonstrating compliance with paragraph 2.c. The required documents, unfolded, must be submitted to the clerk’s office in a sealed envelope marked “HIGHLY SENSITIVE DOCUMENT.” The outside of the envelope must be affixed with a copy of the HSD’s caption page (with confidential information redacted).

c. Service by All Parties

The filing party must serve the motion and proposed HSD on the other parties as provided for in Fed. R. Bankr. P. 7004 and 7005, excluding service via the court’s electronic filing system or any other electronic service.

d. Issuance of Court Order

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 docket entry shall not include personal or other identifying details related to or contained with the HSD. The clerk’s office will maintain the HSD in a secure paper filing system, or a secure standalone computer system not connected to any network.

If the motion is denied, the proposed HSD will be deemed withdrawn and may be retrieved from the clerk’s office by the filing party or counsel within ten calendar days from the date of entry of the order. After ten calendar days, the proposed HSD may be destroyed by the clerk’s office without further notice.

3. Order Granting HSD Designation

- a. An order granting a motion seeking HSD designation, or directing the filing of a document as an HSD on the court’s own motion, must:
 - i. State the identity of the persons who are to have access to the documents without further order of court; and
 - ii. Set forth instructions for the 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.

- b. 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. If the court determines that a court order qualifies as an HSD, the clerk's office will file and maintain the order as an HSD and will serve paper copies of any filing issued by the court.
- c. An HSD in the lower court's record will ordinarily be also regarded by an appellate court as an HSD.

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

- a. 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 and/or a secure standalone computer system not connected to any network.
- b. A party's motion to remove an HSD or highly sensitive case from the court's electronic filing system must explain why such document or case is highly sensitive under the criteria set out in paragraph 1 above or why it should otherwise be subject to the heightened protection for HSDs.

5. Safeguarding Internal Communication:

Care should also be taken 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.

6. 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 info@ganb.uscourts.gov.

IT IS SO ORDERED, this 30th day of April 2024.



BARBARA ELLIS-MONRO
CHIEF UNITED STATES BANKRUPTCY JUDGE

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.