

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLORADO**

**FILING OF HIGHLY  
SENSITIVE DOCUMENTS**

**DISTRICT COURT GENERAL ORDER  
2024-1**

This order supersedes General Order 2022-5.

WHEREAS, federal courts are updating their security procedures to uniformly protect highly sensitive documents, sometimes referred to as “HSDs”, a narrow subset of sealed documents that must, for their protection, be stored outside the Court’s electronic systems;

WHEREAS, good cause exists to permit nonelectronic filing under Fed. R. Civ. P. 5(d)(3)(A) and Fed. R. Crim P. 49(b)(3)(A) and to adopt HSD Guidance, 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; it 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, such as a flash drive), in accordance with this Order and will be maintained by the Clerk’s Office 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). This Order supersedes all prior court orders and inconsistent local rules concerning HSDs.

**1. Documents and Materials Subject to this Order:**

- a. Definition: A Highly Sensitive Document (“HSD”), as the term is used below, 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: *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 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 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. Filing of Motions to Treat a Document as an HSD**

- a. If a case has not been opened, a party intending to file an HSD should proceed as follows:
  - i. Counsel for the filing party shall prepare a motion to treat a document as an HSD and a proposed order in the same manner as a motion to restrict under D.C.COLO.LCrR 47.1 (c ) and D.C.COLO.LCivR 7.2(c). The motion should explain why the proposed document constitutes an HSD under the criteria set out in paragraph 1 above or why it should otherwise be subject to filing protection as an HSD.
  - ii. Counsel for the filing party shall deliver to the criminal duty magistrate judge two paper copies of the motion, proposed order, and HSD. These documents shall be submitted in a sealed envelope marked “HIGHLY SENSITIVE DOCUMENT” along with counsel for the filing party’s name, telephone number, and e-mail address.
  - iii. The presiding judge shall issue an order on the motion. If granted, counsel for the filing party shall then deliver the paperwork to the Clerk’s Office which shall then assign a case number. The Clerk’s Office shall maintain the HSD 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).
- b. If a case has been opened, a party intending to file an HSD should proceed as follows:
  - i. Represented parties:
    - 1) A represented party shall file electronically a motion to treat a document as an HSD and a proposed order in the same fashion as a motion to restrict under D.C.COLO.LCrR 47.1 (c ) and D.C.COLO.LCivR 7.2(c), except that a copy of the proposed HSD shall not be filed electronically. The motion shall explain why the proposed document constitutes an HSD under the criteria set out in paragraph 1 above or why it should otherwise be subject to the filing protection for HSDs. If the motion cannot be filed without revealing the highly sensitivity information contained within the HSD, then the motion should be filed in paper along with the HSD in accordance with paragraph a.ii above.
    - 2) As soon as practicable after the motion is filed, the filing party shall deliver to the Clerk’s Office two paper copies of the HSD along with a certificate of service. These documents shall be submitted in a sealed envelope marked “HIGHLY SENSITIVE DOCUMENT” and marked with the applicable case number, attorney’s name, telephone number, and e-mail address.
    - 3) The filing party shall serve the proposed HSD on the other parties as follows:

- a. Criminal cases – by any manner specified in Fed. R. Crim. P. 49(a)(3)(B) or (a)(4); or
  - b. Civil cases – by any manner specified in Fed. R. Civ. P. 5(b)(2), other than service via the Court’s electronic filing system.
- 4) The presiding judge will issue an order on the motion and, if granted, an informational entry will be made on the docket indicating that the HSD has been filed with the Court. The Clerk’s Office will maintain the HSD 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).
- ii. Pro se parties:
  - 1) Pro se parties authorized to file electronically shall follow the procedures for represented parties outlined above.
  - 2) Pro se parties not authorized to file electronically shall submit to the Clerk’s Office two paper copies of a motion to treat a document as an HSD, the HSD sought to be filed, and a certificate of service. These documents shall be submitted in a sealed envelope marked “HIGHLY SENSITIVE DOCUMENT” and marked with the applicable case number, party’s name, and telephone number.
  - 3) The filing party shall serve the proposed HSD on the other parties as specified in paragraph b.i.3 above.
  - 4) The presiding judge will issue an order on the motion and, if granted, an informational entry will be made on the docket indicating that the HSD has been filed with the Court. The Clerk’s Office will maintain the HSD 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).

### 3. 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, 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 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 a determination, the presiding judge 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.

- c. 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.

#### **4. Orders Granting HSD Designation**

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:

- a. State the identity of the persons who are to have access to the documents without further order of court; and
- b. 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.

If the presiding judge determines that a court order contains highly sensitive information, the Clerk's Office will file and maintain the order to that effect 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). Paper copies of the order will be served on the parties.

#### **5. 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 presiding judge may determine that a document or case 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 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).
- b. A party's motion to remove an HSD or highly sensitive case from the Court's electronic filing system shall 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 filing protection for HSDs.

**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 303-844-3433.

Dated at Denver, Colorado this 4<sup>th</sup> day of June, 2024.

**BY THE COURT**



PHILIP A. BRIMMER  
Chief United States District Judge