# APPENDIX F: HIGHLY SENSITIVE DOCUMENT 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 quality 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.