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

IN RE:	)	
PROCEDURES FOR THE FILING,	)	Misc. No. 21-50
SERVICE, AND MANAGEMENT OF	)	
HIGHLY SENSITIVE DOCUMENTS	)	

ADMINISTRATIVE ORDER

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

THE COURT FINDS that, pursuant to Federal Rule of Civil Procedure 5(d)(3)(A) and Federal Rule of Criminal Procedure 49(b)(3)(A), good cause exists to allow parties to file sealed documents containing HSI outside of the Court's electronic case filing system ("CM/ECF").

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 sealed documents containing HSI is subject to the procedures and requirements set forth below. This Order constitutes authorization to file documents in paper rather than electronic format according to the terms of this Order, notwithstanding the provisions of Local Civil Rule 5.5, Local Criminal Rule 49 or the provisions of the Court's "Electronic Case Filing Policies and Procedures" (including its Paragraph 2), and implements the authorization of Paragraphs 8 and 9.2 of those Policies and Procedures to permit the filing of certain documents in paper format. It supersedes to the extent of this Order all inconsistent provisions in established CM/ECF procedures, or other Orders of this Court. Except as set forth in Paragraph "C" below, the procedures set forth in this Order apply only to sealed documents with HSI filed after the date of this Order. Sealed documents containing HSI shall be known as "highly sensitive documents" ("HSD").

A. Highly Sensitive Documents – General Definition

1. Not all sealed documents contain HSI, and HSI does not refer to all sensitive or confidential information. That a document satisfies the legal criteria for filing under seal is a necessary, but not sufficient, condition for treatment as an HSD. HSI generally refers to sensitive or confidential information that is likely to be of interest to the intelligence service of a hostile foreign government and whose use or disclosure by a hostile foreign government would likely cause significant harm. HSI also includes information contained in documents whose disclosure could jeopardize the safety of specific individuals. Therefore, very few documents filed under seal contain HSI, and documents will not be considered HSDs solely because they include personal identifying information, medical records or information, or financial information about an entity or an individual.

2. The Court anticipates that sealed documents containing HSI will most often be filed in cases involving the following matters:

a. national security;

b. foreign sovereign interests;

c. cybersecurity and cybercrimes;

d. particularly strong domestic or international interests;

e. the reputational interests of the United States;

f. the integrity and functioning of governmental operations; and

g. law-enforcement investigations or intelligence-gathering operations concerning the foregoing.

The Court anticipates that the following types of sealed documents also often contain HSI:

h. Motions setting forth the substantial assistance of a defendant in the investigation or prosecution of another person pursuant to U.S.S.G. § 5K1.1 or Federal Rule of Criminal Procedure 35;

i. Plea agreement supplements detailing terms of cooperation; and

j. Applications and affidavits in support of electronic surveillance under 18 U.S.C. § 2518.

The Court therefore deems all sealed documents containing confidential or sensitive information pertaining to the matters set forth in this paragraph (2) as presumptively containing HSI, and therefore they are deemed HSDs subject to the filing protocol set forth below, without the necessity of a separate order to designate them as HSDs.

3. The following types of documents generally do not contain HSI and therefore are presumptively not considered to be HSDs:

a. Presentence reports, pretrial release reports, and probation violation reports, and documents related to such reports;

b. Social security records, administrative immigration records; and *qui tam* complaints;

c. Commercial or proprietary information; and

d. Most sealed filings in most civil cases.

4. If a party believes that a sealed document contains HSI but does not fall into a category of matters described in paragraph (2), above, the party shall file a motion requesting such relief (without disclosing the HSI) on the docket in CM/ECF using a new event called *Motion for Highly Sensitive Document*. All such motions will be referred to and decided by the presiding judicial officer assigned to the case.

5. Because most sealed filings in civil cases presumptively do not contain HSI, all civil matters must first follow Local Civil Rule 5.2(H) to file a sealed document. If a litigant also believes that the sealed document contains HSI, litigants must also follow the process set forth in paragraph (4), above.

B. Filing of Highly Sensitive Documents (HSDs)

1. Only sealed documents may be considered for designation as HSDs. The filing party must first follow all procedures and protocols currently in place to seek relief from the Court to designate a document as a sealed document. Thereafter, the filing party must determine if it believes that a sealed document also contains HSI.

2. If the filing party believes that a document contains HSI, the filing party must not file the document in the Court's electronic filing system or send the document to the Court through email or any other electronic means (encrypted or otherwise) and, instead, must:

a. Complete the "Highly Sensitive Document Placeholder Form" (the "HSD Placeholder") which is located on the Court's website.

b. If the case is open or will be opened by the filer, file the HSD Placeholder in CM/ECF on the docket of the case in place of the actual HSD using a new event in CM/ECF called *Highly Sensitive Document*.

c. Print a hardcopy of the electronically-filed HSD Placeholder as well as a copy of the Notice of Electronic Filing ("NEF") for the electronically-filed HSD Placeholder.

d. Place the HSD, together with the electronically-filed HSD Placeholder, in a sealed envelope marked "HIGHLY SENSITIVE DOCUMENT" and addressed to the Clerk's Office. Attach the related NEF to the outside of the sealed document envelope. Filers providing a copy of the HSD will be provided with a file-stamped copy of the HSD in-person, by interoffice mail (as may be available), or by return mail when a self-addressed, stamped envelope is provided.

e. Place another copy of the documents set forth in (d), above, in a sealed envelope marked "HIGHLY SENSITIVE DOCUMENT" and addressed to the presiding judicial officer (or, if no judge has been assigned to the case, to the Chief Judge).

f. Contemporaneously with the filing of the HSD Placeholder in CM/ECF, deliver or place in the mail the envelopes to the Clerk's Office and to the Presiding Judicial Officer.

g. In the case of electronic surveillance applications and other Miscellaneous Case matters, the filer must call the Clerk's Office to obtain a case number and additional instruction.

3. When service on other parties is required, the filing party must serve the HSD on other parties as follows:

a. In civil cases: by the manner specified in Federal Rule of Civil Procedure 5(b)(2), except for service via CM/ECF electronic notice;

b. In criminal cases: by the manner specified in Federal Rule of Criminal Procedure 49(a)(3)(B) or (a)(4).

4. 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.

5. If the Court determines that a Court order contains HSI, 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 by U.S. or interoffice mail.

C. Existing Files in CM/ECF

1. Upon motion of a party or upon its own motion, the Court may determine that a document that previously was filed electronically contains HSI and direct that the document or documents (i) be removed from the CM/ECF system and, (ii) be 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. Should a party wish to seek relief under this section, movant should file a motion requesting such relief (without disclosing the HSI) on the docket of the existing case in CM/ECF using a new event called *Motion for Highly Sensitive Document*. All such motions as to cases that are closed on the Court's docket will be referred to and decided by the Judge designated pursuant to Paragraph 8 of the Court's Electronic Case Filing Policies and Procedures to resolve the status of sealed documents. Such a motion shall contain a certification of the movant's good-faith belief that the material contained in the document currently meets the criteria set forth in Section A, above.

2. Any questions about how an HSD should be filed with the Court pursuant to this Administrative Order should be directed to the Clerk's Office at 412-208-7500.

This Order will be effective on January 25, 2021 and will be in effect unless and until it is modified, superseded or vacated by further Order of the undersigned.

Date: January 21, 2021

s/Mark R. Hornak
Mark R. Hornak
Chief United States District Judge