IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN RE:	)	
	)	
PROCEDURES FOR THE FILING,	)	
SERVICE, AND MANAGEMENT OF	)	**Administrative Order No. 286**
HIGHLY SENSITIVE DOCUMENTS.	)	
	)	
	)	

ADMINISTRATIVE ORDER

In response to the recent disclosure of widespread breaches of both private sector and government computer systems as part of what is suspected to be an intelligence-gathering operation by a hostile foreign government, the Judicial Conference has directed all federal courts to immediately add new security procedures to protect sealed documents containing highly sensitive information, referred to hereafter as "highly sensitive documents" or "HSDs."

The Court **FINDS** that, under Federal Rule of Civil Procedure 5(d)(3)(A) and Federal Rule of Criminal Procedure 49(b)(3)(A), good cause exists to require all parties to transmit, file, process, and store HSDs outside of the Court's Case Management/Electronic Case Filing ("CM/ECF") system and computer network systems (including email, scanning, and copying).

IT IS HEREBY ORDERED that, effective as of the date of this Administrative Order and until such time as the Court orders otherwise, the filing of HSDs is subject to the procedures and requirements set forth below. This Administrative Order supersedes all inconsistent provisions in the local rules or other orders of this Court.

A. Highly Sensitive Documents – General Definition and Designation

Highly Sensitive Documents ("HSDs") contain information of a particularly sensitive nature that warrants precautions beyond the sealing mechanism in the judiciary's CM/ECF system – an exclusive subset of sealed documents to prohibit electronic interception.

1. Documents Presumed to be HSDs

The following documents will be designated as HSDs without further court order, and will be submitted, processed, and stored in accordance with procedures prescribed in section B(1) below:

- Applications for search warrants prior to disclosure required by law, and all associated documents filed in any case that contain non-public identifying or substantive information from the HSD warrant application;
- Applications for electronic surveillance (e.g., wiretaps, geolocation tracking, GPS, pen registers, and trap-and-trace), and all associated documents filed in any case that contain non-public identifying or substantive information from the HSD surveillance application; and
- Applications for electronic surveillance under 18 U.S.C. § 2518 prior to disclosure required by law, and all associated documents filed in any case that contain non-public identifying or substantive information from the HSD surveillance application.

2. Motions for HSD Designation

The Court may, on its own motion or on motion of a party pursuant to procedures prescribed in section B(2) below, direct that the following be designated as HSDs.

- Under-seal criminal complaints and/or arrest warrants, where the United States Attorney moves for such designation, for good cause shown;

- Materials whose disclosure could jeopardize national security or place human life or safety at risk; and

- Materials whose disclosure to a foreign power or its agents (as defined by 50 U.S.C. § 1801) would be unlawful under U.S. law or would substantially assist a foreign power or its agents in the development of that foreign power's competing commercial products or products with military applications.

3. Documents Presumed Not to be HSDs

Satisfying the legal criteria for filing under seal is necessary condition, but not solely sufficient to merit treatment as an HSD. Most sealed filings in criminal and civil cases do not constitute HSDs. Documents will not be given HSD status solely because they are *ex parte*, or because they include personal identifying information or financial information about an entity or an individual. Thus, the following documents, for example, will generally not be considered HSDs:

- Presentence reports, pretrial release reports, and probation violation reports;

- Pleadings in criminal cases related to historical cooperation;

- Social Security records; administrative immigration records; and qui tam complaints; and

- Commercial or proprietary information.

B. Filing, Processing, and Storing HSDs

1. Documents Presumed to be HSDs

All documents presumed to be HSDs pursuant to section A(1) above (applications for search warrants or electronic surveillance, and associated documents) will be transmitted, processed, and stored entirely in paper format pursuant to protocols published to the U.S

Attorney's Office. The Clerk's Office will maintain these HSDs in a secure paper filing system or a secure standalone computer system not connected to any network.

2. Motions for HSD Designation and Other HSD-Designated Documents

All motions for HSD designation pursuant to section A(2) above shall be filed as follows:

a. If the filing party determines that a document contains highly sensitive information, the filing party must not file the document in the Court's electronic filing system but must instead:

   i. Complete the "Placeholder Form," which can be found on the Court's website.

   ii. File the Placeholder Form in CM/ECF in place of the sealed document containing highly sensitive information using the applicable CM/ECF event, including adding any applicable parties when filing.

   iii. Print the filed Placeholder Form from CM/ECF as well as a copy of the Notice of Electronic Filing ("NEF") for the Placeholder Form and the sealed document containing highly sensitive information.

   iv. Place the following in a sealed envelope marked "HIGHLY SENSITIVE DOCUMENT" and addressed to the Clerk's Office:
   - A copy of the NEF;
   - A copy of the filed Placeholder Form;
   - The document containing highly sensitive information; and
   - A courtesy copy of all materials.

b. Contemporaneously with filing of the Placeholder Form in CM/ECF; deliver or place in the mail the envelopes to the Clerk's Office.

c. The filing party must serve the sealed document with highly sensitive information on other parties as follows:

   i. Civil cases—by any manner specified in Civil Rule 5(b)(2), except for service via the Court's CM/ECF system; or

   ii. Criminal cases---by any manner specified in Criminal Rule 49(a)(3)(B) or (a)(4).

d. The Clerk's Office will maintain the sealed document with highly sensitive information in a secure paper filing system or a secure standalone computer system that is not connected to any network.

3. Court Review

a. The Court, on motion of a party or its own motion, at any time may review any document to determine the appropriateness of granting or terminating HSD status.

b. If the Court determines that a document that was filed in CM/ECF as a sealed or restricted document must be filed as a sealed HSD, the Clerk's Office will remove the document from the case docket and add an informational entry on the case docket indicating that the document was refiled as a sealed HSD. The Clerk's Office will maintain the sealed HSD in a secure paper filing system or a secure standalone computer system that is not connected to any network.

4. 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 by mail.

5. Questions about HSD Filing Procedures

Any questions about how a sealed document with highly sensitive information should be filed with the Court under this Administrative Order should be directed to the Clerk's Office CM/ECF helpdesk at: ecfhelpdesk@ilsd.uscourts.gov, or (866) 867-3169 (East St. Louis), or (866) 222-2104 (Benton).

IT IS SO ORDERED.

Dated: January 15, 2021

Nancy J. Rosenstengel

NANCY J. ROSENSTENGEL
Chief U.S. District Judge