UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA

UNITED STATES OF AMERICA	**CRIMINAL ACTION**
VERSUS	**NO: [CASE NO.]**
[DEFENDANT]	**SECTION: "[Section]" (4)**

PROTOCOL FOR DISCOVERY OF ESI (CRIMINAL CASE)

Today, most information is created and stored electronically. The advent of electronically stored information (ESI) presents an opportunity for greater efficiency and cost savings for the entire criminal justice system, which is especially important for the representation of indigent defendants. To realize those benefits and to avoid undue cost, disruption, and delay, criminal practitioners must educate themselves and employ best practices for managing ESI discovery.

To promote efficient ESI discovery, the undersigned prepared this protocol as a guide to the parties on issues and considerations that should be given when crafting a discovery protocol in a criminal case.

A. **ESI discovery produced**. The parties should discuss the ESI being produced according to the following general categories:

i. **Investigative materials** (investigative reports, surveillance records, criminal histories, etc.)

ii. **Witness statements** (interview reports, transcripts of prior testimony, Jencks statements, etc.)

iii. **Documentation of tangible objects** (e.g., records of seized items or forensic samples, search warrant returns, etc.)

iv. **Third parties' ESI and digital devices** (computers, phones, hard drives, thumb drives, CDs, DVDs, cloud computing, etc., including forensic images)

v. Photographs and video/audio recordings (crime scene photos; photos of contraband, guns, money; surveillance recordings; surreptitious monitoring recordings; etc.)

vi. **Third-party records and materials** (including those seized, subpoenaed, and voluntarily disclosed)

vii. **Title III wiretap information** (audio recordings, transcripts, line sheets, call reports, court documents, etc.)

viii. **Court records** (affidavits, applications, and related documentation for search and arrest warrants, etc.)

ix. **Tests and examinations**

x. **Experts** (reports and related information)

xi. **Immunity agreements**, plea agreements, and similar materials

xii. **Discovery materials with special production considerations** (such as child pornography, trade secrets, tax return information, etc.)

xiii. **Related matters** (state or local investigative materials, parallel proceedings materials, etc.)

xiv. **Discovery materials available for inspection** but not produced digitally.

B. **Table of contents**. If the producing party has not created a table of contents prior to commencing ESI discovery production, it should consider creating one describing the general categories of information available as ESI discovery. In complex discovery cases, a table of contents to the available discovery materials can help expedite the opposing party's review of discovery, promote early settlement, and avoid discovery disputes, unnecessary expense, and undue delay. Because no single table of contents is appropriate for every case, the producing party may devise a table of contents that is suited to the materials it provides in discovery, its resources, and other considerations.

c. **Forms of production**. The producing party should consider how discoverable materials were provided to it or maintained by the source (e.g., paper or electronic), whether it has converted any materials to a digital format that can be used by the opposing party without disclosing the producing party's work product, and how those factors may affect the production of discovery materials in electronic formats. For particularized guidance see paragraph 6, below. The parties should be flexible in their application of the concept of "maintained by the source." The goals are to retain the ESI's integrity, to allow for reasonable usability, and to reasonably limit costs.

d. **Proprietary or legacy data.** Special consideration should be given to data stored in proprietary or legacy systems, for example, video surveillance recordings in an uncommon format, proprietary databases, or software that is no longer supported by the vendor. The parties should discuss whether a suitable generic-output format or report is available. If a generic output is not available, the parties should discuss the specific requirements necessary to access the data in its original format.

e. **Attorney–client, work product, and protected information issues.** The parties should discuss whether there is privileged, work product, or other protected information in third-party ESI or their own discoverable ESI and should discuss proposed methods and procedures for segregating such information and resolving any disputes.

f. **Confidential and personal information.** The parties should identify and discuss the types of confidential or personal information present in the ESI discovery, appropriate security for that information, and the need for any protective orders or redactions. *See also* section 5(p) below.

g. **Incarcerated defendant.** If the defendant is incarcerated and the court or correctional institution has authorized discovery access in the custodial setting, the parties should consider what institutional requirements or limitations may affect the defendant's access to ESI discovery, such as limitations on hardware or software use.

h. **ESI discovery volume**. To assist in estimating the receiving party's discovery costs and to the extent that the producing party knows the volume of discovery materials it intends to produce immediately or in the future, the producing party may provide such information if such disclosure would not compromise the producing party's interests. Examples of volume include the number of pages of electronic images of paper-based discovery, the volume (e.g., gigabytes) of ESI, the number and aggregate length of any audio or video recordings, and the number and volume of digital devices. Disclosures concerning expected volume are not intended to be so detailed as to require a party to disclose what it intends to produce as discovery before it has a legal obligation to produce the particular discovery material (e.g., Jencks material). Similarly, the parties' estimates are not binding and may not serve as the basis for allegations of misconduct or claims for relief.

i. **Naming conventions and logistics**. The parties should, from the outset of a case, employ naming conventions that would make the production of discovery more efficient. For example, in a Title III wiretap case generally it is preferable that the naming conventions for the audio files, the monitoring logs, and the call transcripts be consistent so that it is easy to cross-reference the audio calls with the corresponding monitoring logs and transcripts. If at the outset of discovery production, a naming convention has not yet been established, the parties should discuss a naming convention before the discovery is produced. The parties should discuss logistics and the sharing of costs or tasks that will enhance ESI production.

J. **Paper materials.** Materials received in paper form may be produced in that form, made available for inspection, or, if they have already been converted to digital format, produced as electronic files that can be viewed and searched.

Three possible methodologies:

i. **Single-page TIFFs.** Production in TIFF and OCR format consists of the following three elements:

(1) Paper documents are scanned to a picture or image that produces one file per page. Documents should be unitized. Each electronic image should be stamped with a unique page label or Bates number.

(2) Text from that original document is generated by OCR and stored in separate text files without formatting in a generic format using the same file naming convention and organization as image file.

(3) Load files that tie together the images and text.

ii. **Multi-page TIFFS.** Production in TIFF and OCR format consists of the following two elements:

(1) Paper documents are scanned to a picture or image that produces one file per document. Each file may have multiple pages. Each page of the electronic image should be stamped with a unique page label or Bates number.

(2) Text from that original document is generated by OCR and stored in separate text files without formatting in a generic format using the same file naming convention and organization as the image file.

iii. **PDF**. Production in multi-page, searchable PDF format consists of the following one element:

(1) Paper documents scanned to a PDF file with text generated by OCR included in the same file. This produces one file per document. Documents should be unitized. Each page of the PDF should be stamped with a unique Bates number.

iv. **Note re: color documents**. Paper documents should not be scanned in color unless the color content of an individual document is particularly significant to the case.

k. **Any software and hardware limitations.** As technology continues to evolve, the parties may have software and hardware constraints on how they can review ESI. Any limitations should be addressed during the meet-and-confer.

l. **ESI from seized or searched third-party ESI digital devices.** When a party produces ESI from a seized or searched third-party digital device (e.g., computer, cell phone, hard drive, thumb drive, CD, DVD, cloud computing, or file share), the producing party should identify the digital device that held the ESI, and, to the extent that the producing party already knows, provide some indication of the device's probable owner or custodian and the location where the device was seized or searched. Where the producing party only has limited authority to search the digital device (e.g., limits set by a search warrant's terms), the parties should discuss the need for protective orders or other mechanisms to regulate the receiving party's access to or inspection of the device.

m. **Inspection of hard drives and/or forensic (mirror) images**. Any forensic examination of a hard drive, whether it is an examination of a hard drive itself or an examination of a forensic image of a hard drive, requires specialized software and expertise. A simple copy of the forensic image may not be sufficient to access the information stored, as specialized software may be needed. The parties should consider how to manage inspection of a hard drive and/or production of a forensic image of a hard drive and what software and expertise will be needed to access the information.

n. **Metadata in third-party ESI.** If a producing party has already extracted metadata from third-party ESI, the parties should discuss whether the producing party should produce the extracted metadata together with an industry-standard load file or, alternatively, produce the files as received by the producing party from the third party. Neither party need undertake additional processing beyond its own case preparation, and both parties are entitled to protect their work product and privileged or other protected information. Because the term "metadata" can encompass different categories of information, the parties should clearly describe what categories of metadata a being discussed, what the producing party has agreed to produce, and any known problems or gaps in the metadata received from third parties.

o. **A reasonable schedule for producing and reviewing ESI.** Because ESI involves complex technical issues, two stages should be addressed. First, the producing party should transmit its ESI in sufficient time to permit reasonable management and review. Second, the receiving party should be proactive about testing the accessibility of the ESI production when it is received. Thus, a schedule should include a date for the receiving party to notify the producing party of any production issues or problems that are impeding use of the ESI discovery.

p. **ESI security**. During the first meet-and-confer, the parties should discuss ESI discovery security and, if necessary, the need for protective orders to prevent unauthorized access to, or disclosure of, ESI discovery that any party intends to share with team members via the Internet or similar system, including:

> i. what discovery material will be produced that is confidential, private, or sensitive, including, but not limited to, grand jury material, witness identifying information, information about informants, a defendant's or co-defendant's personal or business

information, information subject to court protective orders, confidential personal or business information, or privileged information;

ii. whether encryption or other security measures during transmission of ESI discovery are warranted;

iii. what steps will be taken to ensure that only authorized persons have access to the electronically stored or disseminated discovery materials;

iv. what steps will be taken to ensure the security of any website or other electronic repository against unauthorized access;

v. what steps will be taken at the conclusion of the case to remove discovery materials from a website or similar repository; and

vi. what steps will be taken at the conclusion of the case to remove or return ESI discovery materials from the recipient's information system(s), or to securely archive them to prevent unauthorized access.

q. **Other issues.** The parties should address other issues they can anticipate, such as protective orders, "claw-back" agreements between the government and criminal defendant(s), or any issues related to the preservation or collection of ESI discovery. *A "claw-back" agreement outlines procedures to be followed to protect against waiver of privilege or work-product protection due to inadvertent production of documents or data.*

r. **Memorializing agreements.** The parties should memorialize any agreements reached to help forestall later disputes. Additionally, the Court recommends that the agreement between the lawyers be submitted for adoption as an order of the court.

S. **Test runs.** Before producing ESI discovery, a party should consider providing samples of the production format for a test run and, once a format is agreed upon, produce all ESI discovery in that format.

T. **Transmitting ESI Discovery**

a. ESI discovery should be transmitted on electronic media of sufficient size to hold the entire production, for example, a CD, DVD, or thumb drive. If the size of the production warrants a large-capacity hard drive, then the producing party may require the receiving party to bear the cost of the hard drive and to satisfy requirements for the hard drive that are necessary to protect the producing party's IT system from viruses or other harm.

b. The media should be clearly labeled with the case name and number, the producing party, a unique identifier for the media, and a production date.

c. A cover letter should accompany each transmission of ESI discovery providing basic information, including the number of media, the unique identifiers of the media, a brief description of the contents (including a table of contents if created), and any applicable bates ranges or other unique production identifiers. Any necessary passwords to access the content should not be in the cover letter accompanying the data, but in a separate communication.

d. The producing party should retain a write-protected copy of all transmitted ESI as a preserved record to resolve any subsequent disputes.

e. **Email transmission.** When considering transmission of ESI discovery by email, the parties' obligation varies according to the sensitivity of the material, the risk of harm from unauthorized disclosure, and the relative security of email versus alternative transmission. The parties should consider three categories of security:

i. **Not appropriate for email transmission:** Certain categories of ESI discovery are never appropriate for email transmission, including, but not limited to, certain grand jury materials; materials affecting witness safety; materials containing classified, national security, homeland security, tax return, or trade secret information; or other similar items.

ii. **Encrypted email transmission**: Certain categories of ESI discovery warrant encryption or other secure transmission due to their sensitive nature. The parties should discuss and identify those categories in their case. This would ordinarily include, but not be limited to, information about informants, confidential business or personal information, and information subject to court protective orders.

iii. **Unencrypted email transmission:** Other categories of ESI discovery not addressed above may be appropriate for email transmission, but the parties always need to be mindful of their ethical obligations.

U. Consider whether it is necessary to have a plan for managing/returning ESI at the conclusion of the case.

Note:
This protocol is not intended to be an inflexible checklist. It may be adopted in its entirety by the parties or adapted, as appropriate. Not all aspects of this Protocol may be applicable or practical for a particular matter and if the parties do not intend to seek discovery of ESI, it may not be applicable to a particular criminal case.

Karen Wells Roby
Chief U.S. Magistrate Judge