BEST PRACTICES FOR ELECTRONIC DISCOVERY IN CRIMINAL CASES

Western District of Washington
Adopted March 21, 2013

- These best practices reflect recommendations adopted in February 2012 by the Department of Justice and Administrative Office of U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System.

- Lawyers for both the defense and the United States have an obligation to have sufficient technical knowledge and experience (or to have available assistance from those who do) to be able to communicate about electronic discovery, and use the discovery provided. These best practices apply only to the discovery materials that can be produced for examination at a location other than government offices. The best practices do not apply to electronically stored evidence that involves contraband or other particularly sensitive material, such as, images of child pornography or computer hacking software, which will only be made available for inspection in government controlled settings.

- These best practices are designed to encourage parties to meet and confer to identify and resolve problems associated with the production of electronically stored information in the most cost-effective manner to avoid unnecessary duplication of time and expense for all parties, and to avoid unnecessary litigation. The parties are already obligated to confer about discovery under Local Rule CrR 16, and must certify compliance with this obligation before any discovery motion is filed.

- These best practices apply to cases where the volume and nature of the discovery materials increase the complexity of the case. For those cases involving the equivalent of a banker's box or less of documentary materials (if those discovery materials were otherwise available in hard copy), discovery may be produced in any manner that is efficient, and cost effective, and in compliance with the applicable legal discovery obligations.

- These best practices are not intended to alter a party's legal obligations to produce discovery. Those obligations remain the obligations imposed by Federal Rule of Criminal Procedure 16, Rule CrR 16 of the Local Rules for the United States District Court for the Western District of Washington, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland,* and *Giglio v. United States* and their progeny.

- These best practices are not intended to impose requirements on the government to undertake substantial additional processing, incur substantial additional cost, or to

produce material in a particular format that is not already a part of the government's case preparation simply because it is a format desired by an opposing party.

- The terms used throughout best practices have the meanings set out in the attached definitions, which also should guide the parties in their discussions.

Best Practices for the Production of Discovery:

1. General Obligations:

For all cases to which these best practices apply, the parties must meet and confer as soon as possible after a defendant's arraignment to discuss the production of electronic discovery and should use the ESI Discovery Protection Checklist attached as a guide.

A. During this meeting, the parties should discuss the amount of discovery material anticipated and the schedule for the production of these materials.

B. To the extent that the government has not already obtained or created files in a particular electronic format prior to charging, the government will consider any reasonable requests by the defense to produce material in a particular electronic format provided that the production in the requested format does not impose additional costs on the government or require additional staff resources.

i. Where one or more defendants in a case are represented by a Criminal Justice Act (CJA) Panel Attorney, the format in which electronic discovery is produced should either be compatible with the technology requirements adopted for the CJA Panel Attorneys, or be produced with a self-executing program such as I-Publish, unless the CJA attorney agrees to the contrary. A copy of the list of technology requirements for CJA Attorneys is attached to this document.

C. At the discovery conference, the parties must discuss specific issues that might arise in a particular case, including but not limited to (1) whether the case involves materials that should be the subject of a protective order; (2) the production of evidence obtained from hard drives or other seized electronic storage media and the means by which this material can be examined; and (3) the security of electronically seized information where appropriate.

D. At the discovery conference, the parties should discuss whether protective orders can resolve any discovery concerns. For example, in some cases,

protective orders may be used to resolve concerns where the government has received material in native format but has converted the material into a different format in order to perform redactions and the defense requests production of the material in native format.

E. Any specific agreements reached between the parties beyond the requirements of the best practices should be memorialized in a written document.

F. Following the conference, the parties should inform the Court of any problems or issues that are anticipated to arise as a result of the discovery.

G. When discovery is produced, the defense has the obligation to bring to the attention of the government any instances of what are likely production errors and allow reasonable time for the government to correct such problems before the filing of any discovery motion with the Court. Similarly, where the difficulty in reviewing discovery appears to be of a technical nature, as provided in the minimum technology standards for CJA counsel, both government and defense counsel should involve individuals with sufficient technical knowledge in the discussion so that there is clear communication, and misunderstandings of a technical nature can be addressed before the need to resort to motions. As noted above, under Local Rule CrR 16, parties are obligated to confer before a discovery related motion is filed and to attempt to resolve those issues without the involvement of the Court.

2. *Production Formats and Manner of Production:*

In all cases, unless some agreement to the contrary is reached by the parties, the following best practices apply:

A. *Scanned Material*: For documents obtained from non-governmental third parties other than in electronic format, any hard copy discovery that is scanned will be produced in a commonly available format. The format chosen will either be compatible with the minimum technology requirements adopted for the CJA Attorneys (attached), or be produced with a self-executing program such as I-Publish. Where such discovery material has been scanned by the government prior to the return of an indictment or the discovery conference, so long as the format is one that is compatible with the minimum technology requirements for CJA Attorneys or is accompanied with a self-executing program, the government is not obligated to change the format already chosen simply because defense counsel might prefer another format. To the extent that the government has attempted to make the electronic version text searchable for its own purposes, the discovery will be produced in

that format. A text searchable format is preferred to the extent that production of this material in this format is practicable in light of resource constraints and cost.

B. *Material Obtained by the Government in Electronic Format.* In general, where the government has obtained materials from non-governmental third parties in electronic form, such as in "native format," these materials will be produced in the format in which the material was obtained, unless the government has converted that material into a different format to perform redactions, or to permit ease of use. Where such a conversion has occurred, then the material will be produced in any reasonably usable format that is compatible either with the minimum technology requirements adopted for the CJA Attorneys or with a self-executing program. Where the government has converted the material into a different format for purposes of redactions or ease of use, the material will also be preserved in the original format. Where the material has been converted for ease of use, rather than for redaction, at the request of defense counsel, the government will produce the material in the original format in which it was obtained, provided that it does not compromise the integrity of the material. If the material was converted from native format to perform redactions the parties should discuss whether the use of a protective order will resolve any concerns about production of that material in native format.

C. *Text Searchable or Database Material:*

i. The government will make best efforts to have law enforcement agencies provide documents in a text searchable format. As noted above, to the extent that the government has created text searchable electronic files for its own use by the time discovery is provided, the discovery materials should be provided to the defense in that format. Although production in a text searchable format is encouraged, the government is not obligated to create such files if it has not already done so for its own purposes.

ii. To the extent that the government has produced a searchable electronic database, upon request by defense counsel, the government will provide any "load" files that are created for this database. This does not impose on the government the obligation to produce any work product associated with the electronic database. To the extent possible, however, whenever an electronic database is created of discovery materials, efforts should be made to create the database in

such a manner that allows for production of the database without the work product.

D. *Photographs, Video and Audio Files:* To the extent that the government has converted photographs, video or audio recordings into digital format, these items must be produced in that format. The government is not obligated to convert these items into a digital format if it has not done so, or does not intend to do so for purposes of trial.

E. *Wiretap Evidence:* For cases involving wiretap evidence, the government will produce, line sheets (also known as log sheets or monitor summaries) in a text searchable format, and the recordings of the telephone calls in the same format in which they are received from the investigative agency, unless the government has reformatted the material in some way for its own purposes. Where the material has been reformatted, the parties should discuss the format in which the defense would prefer the material. To the extent that the files are provided in something other than a standard format, the government will provide an explanation of the software used to produce the files and instructions on how the files can be reviewed.

i. For foreign language conversations, where defense counsel has agreed that the quality of an initial translation is not a basis for cross-examination, the government will provide working copies of transcripts in translation, or copies of the partial translations once such transcripts or partial transcripts are available, regardless of quality. Prior to any trial, the government will provide a final, quality-checked transcript in a text searchable format. This commitment, however, should not be construed as a commitment to translate and transcribe every call or to translate or transcribe calls at the request of defense counsel. The number of calls transcribed will vary widely based on the nature of the investigation and the nature of the calls.

F. *Hard Drives or Digital Storage Media:* Hard drives or other digital media seized during the execution of a search warrant or obtained in some other fashion may present special problems for discovery which must be addressed during the discovery conference. In some cases, the nature of the contents will be such that the hard drive or digital media will only be made available to the defense for review in a government-controlled laboratory setting. In other cases, even where a mirror image of such evidence is produced, the examination of the evidence may require specialized software and expertise. The parties must confer about how to manage the inspection and examination

of such material or the appropriate forensic image and, in general terms, what software or expertise may be necessary for that purpose. Disclosure of sensitive forensic techniques or software may be an issue and must be addressed on a case-by-case basis.

i. Where the hard drive or digital media has been seized from a party other than the defendant, the parties should discuss the need for protective orders or other approaches to protect the personal identifying information or other personal and sensitive material, unrelated to the case that may be contained on the hard drive.

G. Electronically stored information, (or documents in hard copy that have been scanned into an electronic format) must be produced with identifying "Bates" numbers on each page of the material, or in those cases where the addition of Bates numbers is not technologically possible, contain some other means of uniquely identifying the distinct items. Discovery must be produced with Bates numbers, or alternative identification and file naming conventions that allow for easy identification of the source of documents and the most appropriate organization of the material.

H. A "table of contents" or other appropriate description of the contents must accompany the discovery materials. The purpose of this table of contents is to provide general guidance to the recipient of how the material has been organized, and where broad categories of materials, such as the categories listed as examples below, can be found on the particular storage media. This provision is not intended to impose an obligation on the government to particularize the table of contents for each defendant in a multi-defendant case. Nonetheless, in such cases, the discovery must be produced in a way that identifies for each defense counsel where the criminal history specific to their client and any reports regarding statements made by the client to law enforcement officers may be found. Where the discovery is provided on multiple disks or storage media, the individual disks or storage media should be separately numbered and the table of contents should also indicate on which disk or storage device the particular category of material may be found. Such broad categories include but are not limited to:

i. A report of a defendant's oral statements to a law enforcement officer.
ii. The defendant's criminal history
iii. Investigative reports and materials
iv. Witness statements
v. Tangible Objects

vi. Documents or materials obtained from third parties (whether by subpoena or other means)
vii. Wiretap Line Sheets
viii. Wiretap Audio Recordings
ix. Search Warrants and Supporting Affidavits
x. Applications for Wiretaps
xi. Immunity Agreements and Plea Agreements
xii. Reports regarding Scientific Testing
xiii. Expert reports
xiv. Photographs, Video files and Audio files
xv. Documents seized during the execution of search warrants

I. Where a defendant has been detained pre-trial, to the extent reasonably possible given the format in which the government has obtained the material, the discovery should be provided in a format that permits review within the restrictions that the Bureau of Prisons has placed on access to electronically stored information by pretrial detainees at the Sea-Tac Detention Center. However, where counsel for a defendant has asked for the production of material in a special format that is not compatible with the restrictions the Bureau of Prisons has placed on electronically stored information, and the government has agreed to make the discovery available in the particular format requested, the government is relieved of any obligation to produce an additional set of materials for use by the in-custody defendant. Any conversion of that material to a format that the in-custody defendant can use will then fall on counsel for the defendant.

3. ***Multiple Defendant Cases.***

A. In multiple defendant cases, unless it is obvious from the complaint, relevant affidavits, or the indictment, the Assistant United States Attorneys are encouraged to provide defense counsel with an overview of the particular defendant's role in the case. Such an overview should not be a substitute for the defense review of the discovery materials.

B. In multiple-defendant cases, the defense counsel should confer as soon as possible to determine whether the particular case lends itself to the use of a discovery coordinator. That decision should be made well before pretrial motions cut-off date, to ensure the greatest benefit from the expenditure of CJA funds. If a determination is made that this would be benefit counsel and limit the overall costs a request should be made to the Court for appointment of a discovery coordinator.

DEFINITIONS

To clearly communicate about electronically stored information, it is important that the parties use terms in the same way. Below are common terms used when discussing discovery of electronically stored information:

a. *Cloud computing*. With cloud computing, the user accesses a remote computer hosted by a cloud service provider over the Internet or an intranet to access software programs or create, save, or retrieve data, for example, to send messages or create documents, spreadsheets, or databases. Examples of cloud computing include Gmail, Hotmail, Yahoo! Mail, Facebook, and on-line banking.

b. *Coordinating Discovery Attorney (CDA).* An AOUSC contracted attorney who has technological knowledge and experience, resources, and staff to effectively manage complex ESI in multiple-defendant cases, and who may be appointed by a court in selected multiple-defendant cases to assist CJA panel attorneys and/or FDO staff with discovery management.

c. *Document unitization*. Document unitization is the process of determining where a
document begins (its first page) and ends (its last page), with the goal of accurately describing what was a "unit" as it was received by the party or was kept in the ordinary course of business by the document's custodian. A "unit" includes attachments, for example, an email with an attached spreadsheet. Physical unitization utilizes actual objects such as staples, paper clips and folders to determine pages that belong together as documents. Logical unitization is the process of human review of each individual page in an image collection using logical cues to determine pages that belong together as documents. Such cues can be consecutive page numbering, report titles, similar headers and footers, and other logical cues.

d. *Electronically Stored Information or "ESI."* Any information created, stored, or used with digital technology. Examples include, but are not limited to, word-processing files, e-mail and text messages (including attachments); voicemail; information accessed via the Internet, including social networking sites; information stored on cell phones; information stored on computers, computer systems, thumb drives, flash drives, CDs, tapes, and other digital media, including documents originally obtained in hard copy that have been scanned into an electronic format.

e. *Extracted text.* The text of a native file extracted during ESI processing of the native file, most commonly when native files are converted to TIFF format. Extracted text is more accurate than text created by the OCR processing of

document images that were created by scanning and will therefore provide higher quality search results.

f. *Forensic image (mirror image) of a hard drive or other storage device*. A process that preserves the entire contents of a hard drive or other storage device by creating a bit-by-bit copy of the original data without altering the original media. A forensic examination or analysis of an imaged hard drive requires specialized software and expertise to both create and read the image. User created files, such as email and other electronic documents, can be extracted, and a more complete analysis of the hard drive can be performed to find deleted files and/or access information. A forensic or mirror image is not a physical duplicate of the original drive or device; instead it is a file or set of files that contains all of the data bits from the source device. Thus a forensic or mirror image cannot simply be opened and viewed as if you were looking at the original device. Indeed, forensic or mirror images of multiple hard drives or other storage devices can be stored on a single recipient hard drive of sufficient capacity.

g. *Image of a document or document image.* An electronic "picture" of how the document would look if printed. Images can be stored in various file formats, the most common of which are TIFF and PDF. Document images, such as TIFF and PDF, can be created directly from native files, or created by scanning hard copy.

h. *Load file*. A cross reference file used to import images or data into databases. A data load file may contain Bates numbers, metadata, path to native files, coded data, and extracted or OCR text. An image load file may contain document boundary, image type and path information. Load files must be obtained and provided in software-specific formats to ensure they can be used by the receiving party.

I. *Metadata.* Data that describes characteristics of ESI, for example, the author, date created, and date last accessed of a word processing document. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image. Metadata can describe how, when and by whom ESI was created, accessed, modified, formatted, or collected. Metadata can be supplied by applications, users or the file system, and it can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Metadata is found in different places and in different forms. Some metadata, such as file dates and sizes, can easily be accessed by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Note that some metadata may be lost or changed when an electronic copy of a file is made using ordinary file copy methods.

j. *Native file.* A file as it was created in its native software, for example a Word, Excel, or PowerPoint file, or an email in Outlook or Lotus Notes.

k. *OCR (Optical Character Recognition)*. A process that converts a picture of text into searchable text. The quality of the created text can vary greatly depending on the quality of the original document, the quality of the scanned image, the accuracy of the recognition software and the quality control process of the provider. Generally, OCR does not handle handwritten text or text in graphics well. OCR conversion rates can range from 50 to 98% accuracy depending on the underlying document. A full page of text is estimated to contain 2,000 characters, so OCR software with even 90% accuracy would create a page of text with approximately 200 errors.

l. *Parent - child relationships*. Related documents are described as having a parent/child relationship, for example, where the email is the parent and an attached spreadsheet is the child.

m. *PDF or "Portable Document Format."* A file format created by Adobe that allows a range of options, including electronic transmission, viewing, and searching.

n. *TIFF or "Tagged Image File Format."* An industry-standard file format for storing scanned and other digital black-and-white, gray-scale, and full-color images.

ESI DISCOVERY CHECKLIST

- □ Is this a case where the volume or nature of ESI significantly increases the case's complexity?

- □ Does this case involve classified information?

- □ Does this case involve trade secrets, or national security or homeland security information?

- □ Do the parties have appropriate technical advisors to assist?

- □ Have the parties met and conferred about ESI issues?

- □ Have the parties addressed the format of ESI being produced? Categories may include:

    - ▫ Investigative reports and materials
    - ▫ Witness statements
    - ▫ Tangible objects
    - ▫ Third party ESI digital devices (computers, phones, etc.)
    - ▫ Photos, video and audio recordings
    - ▫ Third party records
    - ▫ Title III wiretap information
    - ▫ Court records
    - ▫ Tests and examinations
    - ▫ Experts
    - ▫ Immunity and plea agreements
    - ▫ Discovery materials with special production considerations
    - ▫ Related matters
    - ▫ Discovery materials available for inspection but not produced digitally
    - ▫ Other information

Have the parties addressed ESI issues involving:

- ▫ Table of contents?
- ▫ Production of paper records as either paper or ESI?
- ▫ Proprietary or legacy data?
- ▫ Attorney-client, work product, or other privilege issues?
- ▫ Sensitive confidential, personal, grand jury, classified, tax return, trade secret, or similar information?

- Whether email transmission is inappropriate for any categories of ESI discovery?
- Incarcerated defendant's access to discovery materials?
- ESI discovery volume for receiving party's planning purposes?
- Parties' software or hardware limitations?
- Production of ESI from 3 party rd digital devices?
- Forensic images of ESI digital devices?
- Metadata in 3rd party ESI?
- Redactions?
- Reasonable schedule for producing party?
- Reasonable schedule for receiving party to give notice of issues?
- Appropriate security measures during transmission of ESI discovery, e.g., encryption?
- Adequate security measures to protect sensitive ESI against unauthorized access or disclosure?
- Need for protective orders, clawback agreements, or similar orders or agreements?
- Collaboration on sharing costs or tasks?
- Need for receiving party's access to original ESI?
- Preserving a record of discovery produced?

□ Have the parties memorialized their agreements and disagreements?

□ Do the parties have a system for resolving disputes informally?

□ Is there a need for a designated discovery coordinator for multiple defendants?

□ Do the parties have a plan for managing/returning ESI at the conclusion of the case