"Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases"

Department of Justice (DOJ) and Administrative Office of the U.S. Courts (AO)
Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG)

February 2012

Introduction to Recommendations for ESI Discovery in Federal Criminal Cases

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.

The Joint Electronic Technology Working Group (JETWG) was created to address best practices for the efficient and cost-effective management of post-indictment ESI discovery between the Government and defendants charged in federal criminal cases. JETWG was established in 1998 by the Director of the Administrative Office of the U.S. Courts (AOUSC) and the Attorney General of the United States. It consists of representatives of the Administrative Office of U.S. Courts' (AOUSC) Office of Defender Services (ODS), the Department of Justice (DOJ), Federal Defender Organizations (FDO), private attorneys who accept Criminal Justice Act (CJA) appointments, and liaisons from the United States Judiciary and other AOUSC offices.

JETWG has prepared recommendations for managing ESI discovery in federal criminal cases, which are contained in the following three documents:

1. **Recommendations for ESI Discovery in Federal Criminal Cases.** The Recommendations provide the general framework for managing ESI, including planning, production, transmission, dispute resolution, and security.

2. **Strategies and Commentary on ESI Discovery in Federal Criminal Cases.** The Strategies provide technical and more particularized guidance for implementing the recommendations, including definitions of terms. The Strategies will evolve in light of changing technology and experience.

3. **ESI Discovery Checklist.** A one-page Checklist for addressing ESI production issues.

The Recommendations, Strategies, and Checklist are intended for cases where the volume and/or nature of the ESI produced as discovery significantly increases the complexity of the case. They are not intended for all cases. The Recommendations, Strategies, and Checklist build upon the following basic principles:

Principle 1: Lawyers have a responsibility to have an adequate understanding of electronic discovery. (See #4 of the Recommendations.)

Principle 2: In the process of planning, producing, and resolving disputes about ESI discovery, the parties should include individuals with sufficient technical knowledge and experience regarding ESI. (See #4 of the Recommendations.)

Principle 3: At the outset of a case, the parties should meet and confer about the nature, volume, and mechanics of producing ESI discovery. Where the ESI discovery is particularly complex or produced on a rolling basis, an on-going dialogue may be helpful. (See #5 of the Recommendations and Strategies.)

Principle 4: The parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should maintain the ESI's

integrity, allow for reasonable usability, reasonably limit costs, and, if possible, conform to industry standards for the format. (See #6 of the Recommendations and Strategies.)

Principle 5: When producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production. (See #6 of the Recommendations and Strategies.)

Principle 6: Following the meet and confer, the parties should notify the court of ESI discovery production issues or problems that they reasonably anticipate will significantly affect the handling of the case. (See #5(s) of the Strategies.)

Principle 7: The parties should discuss ESI discovery transmission methods and media that promote efficiency, security, and reduced costs. The producing party should provide a general description and maintain a record of what was transmitted. (See #7 of the Recommendations and Strategies.)

Principle 8: In multi-defendant cases, the defendants should authorize one or more counsel to act as the discovery coordinator(s) or seek appointment of a Coordinating Discovery Attorney. (See #8 of the Recommendations and Strategies.)

Principle 9: The parties should make good faith efforts to discuss and resolve disputes over ESI discovery, involving those with the requisite technical knowledge when necessary, and they should consult with a supervisor, or obtain supervisory authorization, before seeking judicial resolution of an ESI discovery dispute or alleging misconduct, abuse, or neglect concerning the production of ESI. (See #9 of the Recommendations.)

Principle 10: All parties should limit dissemination of ESI discovery to members of their litigation team who need and are approved for access, and they should also take reasonable and appropriate measures to secure ESI discovery against unauthorized access or disclosure. (See #10 of the Recommendations.)

The Recommendations, Strategies, and Checklist set forth a collaborative approach to ESI discovery involving mutual and interdependent responsibilities. The goal is to benefit all parties by making ESI discovery more efficient, secure, and less costly.

Recommendations for ESI Discovery Production in Federal Criminal Cases

1. Purpose

These Recommendations are intended to promote the efficient and cost-effective post-indictment production of electronically stored information (ESI) in discovery[1] between the Government and defendants charged in federal criminal cases, and to reduce unnecessary conflict and litigation over ESI discovery by encouraging the parties to communicate about ESI discovery issues, by creating a predictable framework for ESI discovery, and by establishing methods for resolving ESI discovery disputes without the need for court intervention.

ESI discovery production involves the balancing of several goals:

a) the parties must comply with their legal discovery obligations;

b) the volume of ESI in many cases may make it impossible for counsel to personally review every potentially discoverable item, and, as a consequence, the parties increasingly will employ software tools for discovery review, so ESI discovery should be done in a manner to facilitate electronic search, retrieval, sorting, and management of discovery information;

c) the parties should look for ways to avoid unnecessary duplication of time and expense for both parties in the handling and use of ESI;

d) subject to subparagraph (e), below, the producing party should produce its ESI discovery materials in industry standard formats;

e) the producing party is not obligated to undertake additional processing desired by the receiving party that is not part of the producing party's own case preparation or discovery production[2]; and

f) the parties must protect their work product, privileged, and other protected information.

The following Recommendations are a general framework for informed discussions between the parties about ESI discovery issues. The efficient and cost-effective production of ESI discovery materials is enhanced when the parties communicate early and regularly about any ESI discovery issues in their

---

[1] The Recommendations and Strategies are intended to apply only to disclosure of ESI under Federal Rules of Criminal Procedure 16 and 26.2, *Brady*, *Giglio*, and the Jencks Act, and they do not apply to, nor do they create any rights, privileges, or benefits during, the gathering of ESI as part of the parties' criminal or civil investigations. The legal principles, standards, and practices applicable to the discovery phase of criminal cases serve different purposes than those applicable to criminal and civil investigations.

[2] One example of the producing party undertaking additional processing for its discovery production is a load file that enables the receiving party to load discovery materials into its software.

case, and when they give the court notice of ESI discovery issues that will significantly affect the handling of the case.

2. Scope: Cases Involving Significant ESI

No single approach to ESI discovery is suited to all cases. These Recommendations are intended for cases where the volume and/or nature of the ESI produced as discovery significantly increases the complexity of the case.[3] In simple or routine cases, the parties should provide discovery in the manner they deem most efficient in accordance with the Federal Rules of Criminal Procedure, local rules, and custom and practice within their district.

Due to the evolving role of ESI in criminal cases, these Recommendations and the parties' practices will change with technology and experience. As managing ESI discovery becomes more routine, it is anticipated that the parties will develop standard processes for ESI discovery that become the accepted norm.

3. Limitations

These Recommendations and the accompanying Strategies do not alter the parties' discovery obligations or protections under the U.S. Constitution, the Federal Rules of Criminal Procedure, the Jencks Act, or other federal statutes, case law, or local rules. They may not serve as a basis for allegations of misconduct or claims for relief and they do not create any rights or privileges for any party.

4. Technical Knowledge and Experience

For complex ESI productions, each party should involve individuals with sufficient technical knowledge and experience to understand, communicate about, and plan for the orderly exchange of ESI discovery. Lawyers have a responsibility to have an adequate understanding of electronic discovery.

5. Planning for ESI Discovery Production - The Meet and Confer Process

At the outset of a case involving substantial or complex ESI discovery, the parties should meet and confer about the nature, volume, and mechanics of producing ESI discovery. The parties should determine how to ensure that any "meet and confer" process does not run afoul of speedy trial deadlines. Where the ESI discovery is particularly complex or produced on a rolling basis, an on-going dialogue during the discovery phase may be helpful. In cases where it is authorized, providing ESI discovery to an incarcerated defendant presents challenges that should be discussed early. Also, cases involving classified information will not fit within the Recommendations and Strategies due to the unique legal procedures applicable to those cases. ESI that is contraband (*e.g.,* child pornography) requires special discovery procedures. The Strategies and Checklist provide detailed recommendations on planning for ESI discovery.

---

[3] Courts and litigants will continue to seek ways to identify cases deserving special consideration. While the facts and circumstances of cases will vary, some factors may include: (1) a large volume of ESI; (2) unique ESI issues, including native file formats, voluminous third-party records, non-standard and proprietary software formats; and/or (3) multiple defendant cases accompanied by a significant volume of ESI.

6. Production of ESI Discovery

Production of ESI discovery involves varied considerations depending upon the ESI's source, nature, and format. Unlike certain civil cases, in criminal cases the parties generally are not the original custodian or source of the ESI they produce in discovery. The ESI gathered by the parties during their investigations may be affected or limited by many factors, including the original custodian's or source's information technology systems, data management practices, and resources; the party's understanding of the case at the time of collection; and other factors. Likewise, the electronic formats used by the parties for producing ESI discovery may be affected or limited by several factors, including the source of the ESI; the format(s) in which the ESI was originally obtained; and the party's legal discovery obligations, which may vary with the nature of the material. The Strategies and Checklist provide detailed recommendations on production of ESI discovery.

General recommendations for the production of ESI discovery are:

a. The parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should, if possible, conform to industry standards for the format.[4]

b. ESI received from third parties should be produced in the format(s) it was received or in a reasonably usable format(s). ESI from the government's or defendant's business records should be produced in the format(s) in which it was maintained or in a reasonably usable format(s).

c. Discoverable ESI generated by the government or defense during the course of their investigations (*e.g.,* investigative reports, witness interviews, demonstrative exhibits, etc.) may be handled differently than in 6(a) and (b) above because the parties' legal discovery obligations and practices vary according to the nature of the material, the applicable law, evolving legal standards, the parties' policies, and the parties' evolving technological capabilities.

d. When producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production. For example, the producing party need not convert ESI from one format to another or undertake additional processing of ESI beyond what is required to satisfy its legal disclosure obligations. If the receiving party desires ESI in a condition different from what the producing party intends to produce, the parties should discuss what is reasonable in terms of expense and mechanics, who will bear the burden of any additional cost or work, and how to protect the producing party's work product or privileged information. Nonetheless, with the understanding that in certain instances the results of processing ESI may constitute work product not subject to discovery, these

[4] An example of "format of production" might be TIFF images, OCR text files, and load files created for a specific software application. Another "format of production" would be native file production, which would accommodate files with unique issues, such as spreadsheets with formulas and databases. ESI in a particular case might warrant more than one format of production depending upon the nature of the ESI.

recommendations operate on the general principle that where a producing party elects to engage in processing of ESI, the results of that processing should, unless they constitute work product, be produced in discovery along with the underlying ESI so as to save the receiving party the expense of replicating the work.

7. Transmitting ESI Discovery

The parties should discuss transmission methods and media that promote efficiency, security, and reduce costs. In conjunction with ESI transmission, the producing party should provide a general description and maintain a record of what was transmitted. Any media should be clearly labeled. The Strategies and Checklist contain detailed recommendations on transmission of ESI discovery, including the potential use of email to transmit ESI.

8. Coordinating Discovery Attorney

In cases involving multiple defendants, the defendants should authorize one or more counsel to act as the discovery coordinator(s) or seek the appointment of a Coordinating Discovery Attorney[5] and authorize that person to accept, on behalf of all defense counsel, the ESI discovery produced by the government. Generally, the format of production should be the same for all defendants, but the parties should be sensitive to different needs and interests in multiple defendant cases.

9. Informal Resolution of ESI Discovery Matters

a. Before filing any motion addressing an ESI discovery issue, the moving party should confer with opposing counsel in a good-faith effort to resolve the dispute. If resolution of the dispute requires technical knowledge, the parties should involve individuals with sufficient knowledge to understand the technical issues, clearly communicate the problem(s) leading to the dispute, and either implement a proposed resolution or explain why a proposed resolution will not solve the dispute.

b. The Discovery Coordinator within each U.S. Attorney's Office should be consulted in cases presenting substantial issues or disputes.

---

[5] Coordinating Discovery Attorneys (CDA) are AOUSC contracted attorneys who have technological knowledge and experience, resources, and staff to effectively manage complex ESI in multiple defendant cases. The CDAs may be appointed by the court to provide in-depth and significant hands-on assistance to CJA panel attorneys and FDO staff in selected multiple-defendant cases that require technology and document management assistance. They can serve as a primary point of contact for the U.S. Attorneys Office to discuss ESI production issues for all defendants, resulting in lower overall case costs for the parties. If a panel attorney or FDO is interested in utilizing the services of the CDA, they should contact the National Litigation Support Administrator or Assistant National Litigation Support Administrator for the Office of Defender Services at 510-637-3500.

c. To avoid unnecessary litigation, prosecutors and Federal Defender Offices[6] should institute procedures that require line prosecutors and defenders (1) to consult with a supervisory attorney before filing a motion seeking judicial resolution of an ESI discovery dispute, and (2) to obtain authorization from a supervisory attorney before suggesting in a pleading that opposing counsel has engaged in any misconduct, abuse, or neglect concerning production of ESI.

d. Any motion addressing a discovery dispute concerning ESI production should include a statement of counsel for the moving party relating that after consultation with the attorney for the opposing party the parties have been unable to resolve the dispute without court action.

10. Security: Protecting Sensitive ESI Discovery from Unauthorized Access or Disclosure

Criminal case discovery entails certain responsibilities for all parties in the careful handling of a variety of sensitive information, for example, grand jury material, the defendant's records, witness identifying information, information about informants, information subject to court protective orders, confidential personal or business information, and privileged information. With ESI discovery, those responsibilities are increased because ESI is easily reproduced and disseminated, and unauthorized access or disclosure could, in certain circumstances, endanger witness safety; adversely affect national security or homeland security; leak information to adverse parties in civil suits; compromise privacy, trade secrets, or classified, tax return, or proprietary information; or prejudice the fair administration of justice. The parties' willingness to produce early, accessible, and usable ESI discovery will be enhanced by safeguards that protect sensitive information from unauthorized access or disclosure.

All parties should limit dissemination of ESI discovery to members of their litigation team who need and are approved for access. They should also take reasonable and appropriate measures to secure ESI discovery against unauthorized access or disclosure.

During the initial meet and confer and before ESI discovery is produced, the parties should discuss whether there is confidential, private or sensitive information in any ESI discovery they will be providing. If such information will be disclosed, then the parties should discuss how the recipients will prevent unauthorized access to, or disclosure of, that ESI discovery, and, absent agreement on appropriate security, the producing party should seek a protective order from the court addressing management of the particular ESI at issue. The producing party has the burden to raise the issue anew if it has concerns about any ESI discovery it will provide in subsequent productions. The parties may choose to have standing agreements so that their practices for managing ESI discovery are not discussed in each case. The Strategies contains additional guidance in sections 5(f), 5(p), and 7(e).

[6] For private attorneys appointed under the Criminal Justice Act (CJA), this subsection (c) is not applicable.

Strategies and Commentary on ESI Discovery in Federal Criminal Cases

1. Purpose

This commentary contains strategies for implementing the ESI discovery Recommendations and specific technical guidance. Over time it will be modified in light of experience and changing technology. Definitions of common ESI terms are provided in paragraph 11, below.

2. Scope of ESI Gathered

In order to promote efficiency and avoid unnecessary costs, when gathering ESI the parties should take into consideration the nature, volume, and mechanics of managing ESI.

3. Limitations

Nothing contained herein creates any rights or privileges for any party.

4. Technical Knowledge and Experience

No additional commentary.

5. Planning for ESI Discovery Production - The Meet and Confer Process

To promote efficient ESI discovery, the parties may find it useful to discuss the following:

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 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 wire tap 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**

xv. **Other information**

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.[1] 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.[2]

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

---

[1] *See, e.g., U.S. v. Skilling*, 554 F.3d 529, 577 (5th Cir. 2009) (no *Brady* violation where government disclosed several hundred million page database with searchable files and produced set of hot documents and indices).

[2] A table of contents is intended to be a general, high-level guide to the categories of ESI discovery. Because a table of contents may not be detailed, complete, or free of errors, the parties still have the responsibility to review the ESI discovery produced. With ESI, particular content usually can be located using available electronic search tools. There are many ways to construct a general table of contents. For example, a table of contents could be a folder structure as set forth above in paragraph 2(a)(i-xv), where like items are placed into folders.

of "maintained by the source." The goals are to retain the ESI's integrity, to allow for reasonable usability, and to reasonably limit costs.[3]

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**.[4] The parties should discuss whether there is privileged, work product, or other protected information in third-party ESI or their own discoverable ESI and proposed methods and procedures for segregating such information and resolving any disputes.[5]

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.[6]

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.

---

[3] For example, when the producing party processes ESI to apply Bates numbers, load it into litigation software, create TIFF images, etc., the ESI is slightly modified and no longer in its original state. Similarly, some modification of the ESI may be necessary and proper in order to allow the parties to protect privileged information, and the processing and production of ESI in certain formats may result in the loss or alteration of some metadata that is not significant in the circumstances of the particular case.

[4] Attorney-client and work product (*see, e.g.,* F.R.Crim.P. 16(a)(2) and (b)(2)) issues arising from the parties' own case preparation are beyond the scope of these Recommendations, and they need not be part of the meet and confer discussion.

[5] If third party records are subject to an agreement or court order involving a selective waiver of attorney-client or work product privileges (*see* F.R.E. 502), then the parties should discuss how to handle those materials.

[6] Because pretrial detainees often are held in local jails (for space, protective custody, cost, or other reasons) that have varying resources and security needs, there are no uniform practices or rules for pretrial detainees' access to ESI discovery. Resolution of the issues associated with such access is beyond the scope of the Recommendations and Strategies.

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 they intend to produce as discovery before they have 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 wire tap 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.** For options and particularized guidance on paper materials *see* paragraphs 6(a) and(e), below.

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.[7] 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 are 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 pro-active 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;[8]

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 the 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.

---

[7] The producing party is, of course, limited to what it received from the third party. The third party's processing of the information can affect or limit what metadata is available.

[8] The parties should consult their litigation support personnel concerning encryption or other security options.

Note: Because all parties want to ensure that ESI discovery is secure, the Department of Justice, Federal Defender Offices, and CJA counsel are compiling an evolving list of security concerns and recommended best practices for appropriately securing discovery. Prosecutors and defense counsel with security concerns should direct inquiries to their respective ESI liaisons[9] who, in turn, will work with their counterparts to develop best practice guidance.

q. **Other issues.** The parties should address other issues they can anticipate, such as protective orders, "claw-back" agreements[10] between the government and criminal defendant(s), or any issues related to the preservation or collection of ESI discovery.

r. **Memorializing agreements.** The parties should memorialize any agreements reached to help forestall later disputes.

s. **Notice to court.**

i. *Preparing for the meet and confer:* A defendant who anticipates the need for technical assistance to conduct the meet and confer should give the court adequate advance notice if it will be filing an *ex parte* funds request for technical assistance.

ii. *Following the meet and confer:* The parties should notify the court of ESI discovery production issues or problems that they anticipate will significantly affect when ESI discovery will be produced to the receiving party, when the receiving party will complete its accessibility assessment of the ESI discovery received,[11] whether the receiving party will need to make a request for supplemental funds to manage ESI discovery, or the scheduling of pretrial motions or trial.

6. **Production of ESI Discovery**

a. **Paper Materials.** Materials received in paper form may be produced in that form,[12] made available for inspection, or, if they have already been converted to digital format,

---

[9] Federal Defender Organizations and CJA panel attorneys should contact Sean Broderick (National Litigation Support Administrator) or Kelly Scribner (Assistant National Litigation Support Administrator) at 510-637-3500, or by email: sean_broderick@fd.org, kelly_scribner@fd.org. Prosecutors should contact Andrew Goldsmith (National Criminal Discovery Coordinator) at Andrew.Goldsmith@usdoj.gov or John Haried (Assistant National Criminal Discovery Coordinator) at John.Haried@usdoj.gov.

[10] 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.

[11] *See* paragraph 5(o) of the Strategies, above.

[12] The decision whether to scan paper documents requires striking a balance between resources (including personnel and cost) and efficiency. The parties should make that determination on a case-by-case basis.

produced as electronic files that can be viewed and searched. Methods are described below in paragraph 6(b).

b. **Electronic production of paper documents.** 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.[13]

c. **ESI production.** Three possible methodologies:

---

[13] Color scanning substantially slows the scanning process and creates huge electronic files which consume storage space, making the storage and transmission of information difficult. An original signature, handwritten marginalia in blue or red ink, and colored text highlights are examples of color content that may be particularly significant to the case.

i. *Native files as received.* Production in a native file format without any processing consists of a copy of ESI files in the same condition as they were received.

ii. *ESI converted to electronic image.* Production of ESI in a TIFF or PDF and extracted text format consists of the following four elements:

(1) Electronic documents converted from their native format into a picture / image. The electronic image files should be computer generated, as opposed to printed and then imaged. Each electronic image should be stamped with a unique Bates number.

(2) Text from that original document is extracted or pulled out and stored without formatting in a generic format.

(3) Metadata (*i.e.,* information about that electronic document), depending upon the type of file converted and the tools or methodology used, that has been extracted and stored in an industry standard format. The metadata must include information about structural relationships between documents, *e.g.,* parent-child relationships.

(4) Load files that tie together the images, text, and metadata.

iii. *Native files with metadata.* Production of ESI in a processed native file format consists of the following four elements:

(1) The native files.

(2) Text from that original document is extracted or pulled out and stored without formatting in a generic format.

(3) Metadata (*i.e.,* information about that electronic document), depending upon the type of file converted and the tools or methodology used, that has been extracted and stored in an industry standard format. The metadata must include information about structural relationships between documents, *e.g.,* parent-child relationships.

(4) Load files that tie together the native file, text, and metadata.

d. **Forensic images of digital media.** Forensic images of digital media should be produced in an industry-standard forensic format, accompanied by notice of the format used.

e. **Printing ESI to paper.** The producing party should not print ESI (including TIFF images or PDF files) to paper as a substitute for production of the ESI unless agreed to by the parties.

f. **Preservation of ESI materials received from third parties**. A party receiving potentially discoverable ESI from a third party should, to the extent practicable, retain a copy of the

ESI as it was originally produced in case it is subsequently needed to perform quality control or verification of what was produced.

g. **Production of ESI from third parties.** ESI from third parties may have been received in a variety of formats, for example, in its original format (native, such as Excel or Word), as an image (TIFF or PDF), as an image with searchable text (TIFF or PDF with OCR text), or as a combination of any of these. The third party's format can affect or limit the available options for production as well as what associated information (metadata) might be available. ESI received from third parties should be produced in the format(s) it was received or in a reasonably usable format(s). ESI received from a party's own business records should be produced in the format(s) in which it was maintained or in a reasonably usable form(s). The parties should explore what formats of production[14] are possible and appropriate, and discuss what formats can be generated. Any format selected for producing discovery should, if possible and appropriate, conform to industry standards for the format.

h. **ESI generated by the government or defense.** Paragraphs 6(f) and 6(g) do not apply to discoverable materials generated by the government or defense during the course of their investigations (*e.g.,* demonstrative exhibits, investigative reports and witness interviews - *see* subparagraph i, below, etc.) because the parties' legal discovery obligations and practices vary according to the nature of the material, the applicable law, evolving legal standards, and the parties' evolving technological capabilities. Thus, such materials may be produced differently from third party ESI. However, to the extent practicable, this material should be produced in a searchable and reasonably usable format. Parties should consult with their investigators in advance of preparing discovery to ascertain the investigators' ESI capabilities and limitations.

i. **Investigative reports and witness interviews.** Investigative reports and witness interviews may be produced in paper form if they were received in paper form or if the final version is in paper form. Alternatively, they may be produced as electronic images (TIFF images or PDF files), particularly when needed to accommodate any necessary redactions. Absent particular issues such as redactions or substantial costs or burdens of additional processing, electronic versions of investigative reports and witness interviews should be produced in a searchable text format (such as ASCII text, OCR text, or plain text (.txt)) in order to avoid the expense of reprocessing the files. To the extent possible, the electronic image files of investigative reports and witness interviews should be computer-generated (as opposed to printed to paper and then imaged) in order to produce a higher-quality searchable text which will enable the files to be more easily searched and cost-effectively utilized.[15]

---

[14] An example of "format of production" might be TIFF images, OCR text files, and load files created for a specific software application. Another "format of production" would be native file production, which would accommodate files with unique issues, such as spreadsheets with formulas and databases.

[15] For guidance on making computer generated version of investigative reports and witness interview reports, *see* the description of production of TIFF, PDF, and extracted text format in paragraphs 6(b)(ii)(1) and (ii).

j. **Redactions**. ESI and/or images produced should identify the extent of redacted material and its location within the document.

k. **Photographs and video and audio recordings**. A party producing photographs or video or audio recordings that either were originally created using digital devices or have previously been digitized should disclose the digital copies of the images or recordings if they are in the producing party's possession, custody or control. When technically feasible and cost-efficient, photographs and video and audio recordings that are not already in a digital format should be digitized into an industry standard format if and when they are duplicated. The producing party is not required to convert materials obtained in analog format to digital format for discovery.

l. **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.

m. **Access to originals.** If the producing party has converted paper materials to digital files, converted materials with color content to black and white images, or processed audio, video, or other materials for investigation or discovery, it should provide reasonable access to the originals for inspection and/or reprocessing.

7. 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.[16] 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, any applicable bates ranges or other unique production identifers, and any necessary passwords to access the content. Passwords 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

[16] Rolling productions may, of course, use multiple media. The producing party should avoid using multiple media when a single media will facilitate the receiving party's use of the material.

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 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.[17]

8. Coordinating Discovery Attorney

Coordinating Discovery Attorneys (CDA) are AOUSC contracted attorneys who have technological knowledge and experience, resources, and staff to effectively manage complex ESI in multiple defendant cases. The CDAs may be appointed by the court to provide additional in-depth and significant hands-on assistance to CJA panel attorneys and FDO staff in selected multiple-defendant cases that require technology and document management assistance. They can serve as a primary point of contact for the US Attorneys Office to discuss ESI production issues for all defendants, resulting in lower overall case costs for the parties. If you have any questions regarding the services of a CDA, please contact either Sean Broderick (National Litigation Support Administrator) or Kelly Scribner (Assistant National Litigation Support Administrator) at 510-637-3500, or by email: sean_broderick@fd.org, kelly_scribner@fd.org.

9. Informal Resolution of ESI Discovery Matters

No additional commentary.

10. Security: Protecting Sensitive ESI Discovery from Unauthorized Access or Disclosure

See sections 5(f) - Confidential and personal information, 5(p) - ESI security, and 7(e) - Email Transmission of the Strategies for additional guidance.

[17] Illustrative of the security issues in the attorney-client context are ABA Op. 11-459 (Duty to Protect the Confidentiality of E-mail Communications with One's Client) and ABA Op. 99-413 (Protecting the Confidentiality of Unencrypted E-Mail).

11. Definitions

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

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. **ESI (Electronically Stored Information).** Any information created, stored, or utilized 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.

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

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

ESI Discovery Production 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 wire tap 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 3rd party 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?