

MEMORANDUM

TO: United States District Court for the Western District of Missouri

FROM: ESI Committee

DATE: August 9, 2016

RE: Proposed Principles and Recommendations for Managing Electronic Discovery in Criminal Cases

The ESI Committee recommends that the Court consider adopting the attached proposed Principles and Recommendations for Managing the Discovery of Electronically Stored Information (ESI) in Criminal Cases.

This recommendation was vetted through the Federal Practice Committee and positively received with no further changes suggested.

The Historical Development of Best Practices for E-Discovery in Criminal Cases

In an effort to develop best practices for the efficient and cost-effective management of post-indictment e-discovery in federal criminal cases, the Director of the Administrative Office of the U.S. Courts (AOUSC) and the Attorney General of the United States established the Joint Electronic Technology Working Group (JETWG) in 1998. The JETWG includes representatives from the AOUSC's 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. In 2012, the JETWG produced what has since become known as the ESI Protocol, a comprehensive set of recommended best practices for e-discovery production in federal criminal cases.¹ Because it was produced collaboratively by seasoned defense and prosecution practitioners, the ESI Protocol has been widely accepted and recognized as authoritative. The DOJ trains its prosecutors to use the ESI Protocol in cases involving complex e-discovery, and most federal defenders and CJA attorneys have received similar training on the ESI Protocol.

In 2015, the Federal Judicial Center published a pamphlet entitled *Criminal e-Discovery: A Pocket Guide for Judges*.² The *Pocket Guide*, developed at the request of the federal judiciary, also was a collaborative project involving representatives from the DOJ, the ODS, FDO, CJA panel attorneys, and the Federal Judicial Center. The *Pocket Guide* discusses e-discovery challenges and how the ESI Protocol can help lawyers and judges identify and resolve various e-discovery issues. It also contains suggested colloquies for judges who want to engage defense counsel and prosecutors on e-discovery matters.

¹Online at: <https://www.fd.org/docs/litigation-support/final-esi-protocol.pdf>

²Online at: [http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/\\$file/Criminal-e-Discovery.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/$file/Criminal-e-Discovery.pdf).

The groundwork laid by the ESI Protocol and the *Pocket Guide* means that the Court can confidently rely on them as collaborative, comprehensive, and nationally applicable guidance in developing best practices and principles for managing e-discovery in criminal cases in the Western District of Missouri. Indeed, several other districts have already done so.³

Benefits of Adopting the Recommended Principles and Recommendations

We are undeniably living in an electronic information age. The burdens associated with the production and review of ESI in criminal discovery is ever growing. As we look to the future, the volume of ESI produced as discovery in criminal cases will only increase. By adopting principles and recommendations for managing e-discovery in criminal cases, the Court acknowledges the impact of ESI in criminal cases and signals its commitment to managing e-discovery in a way that promotes the efficient administration of the criminal justice process.

Specifics of the Proposed Principles and Recommendations

The Principles and Recommendations for Managing Discovery of ESI in Criminal Cases proposed by the ESI Committee are solidly based on the ESI Protocol and the *Pocket Guide* and are, in essence, a condensed version of the ESI Protocol. Instead of a twenty-plus page ESI Protocol, the proposal is only six total pages, including a single page appendix devoted to basic technology requirements that an attorney practicing criminal law should typically possess, and a two page checklist, borrowed directly from the ESI Protocol, for practitioners to use when producing and distributing e-discovery.

Unlike the local civil rules in the Western District of Missouri, there are very few local criminal rules and none of them addresses e-discovery. The proposed principles and recommendations therefore introduce the use of practices that have not been formally undertaken as a matter of course in criminal cases in the past, e.g., the recommendation that the parties meet and confer as soon as possible after arraignment to address any issues associated with the production of ESI.

The ESI Committee recommends adoption of the proposed principles and recommendations because, like the ESI Protocol, they are intended to: (1) promote the efficient and cost-effective post-indictment production of ESI in federal criminal cases, and (2) reduce unnecessary conflict and litigation over e-discovery by encouraging the parties to discuss issues. The proposed principles and recommendations accomplish these goals by creating a predictable framework for e-discovery and establishing methods for resolving e-discovery disputes.

The ESI Committee considered whether to recommend adoption of a new local criminal rule(s) incorporating these principles and recommendations. However, the general view of the Committee was that the Court, on its own, can consider whether it should implement a new local criminal rule.

³For example, the District of New Hampshire website provides a [link](#) to the ESI Protocol. The Northern District of Georgia website provides a similar [link](#) to the ESI Protocol. The Western District of Washington has adopted [Best Practices for Electronic Discovery in Criminal Cases](#) that are based on the ESI Protocol. The Northern District of California website has a [page](#) devoted to the ESI Protocol.

United States District Court
Western District of Missouri

PRINCIPLES AND RECOMMENDATIONS FOR
MANAGING DISCOVERY OF ELECTRONICALLY STORED INFORMATION IN
CRIMINAL CASES¹

These principles and recommendations are intended to promote the efficient and cost-effective post-indictment production of electronically stored information (ESI) in discovery² between the Government and defendants charged in federal criminal cases. Their goal is to reduce unnecessary conflict and litigation over ESI by encouraging the parties to communicate about e-discovery issues by creating a predictable framework for e-discovery and establishing methods for resolving e-discovery disputes without the need of court intervention.³

Principle 1 (Technology Competence)

Attorneys should have an adequate understanding of e-discovery and the associated technology. The Court expects attorneys to have sufficient technical knowledge and experience (or to involve individuals with sufficient technical knowledge and experience) to be able to understand, communicate about, plan for, and review e-discovery. Because discoverable information is increasingly found and produced electronically, the Court strongly encourages attorneys to be familiar with and to have access to the technology set forth in Appendix A. In the process of planning, producing, and resolving e-discovery disputes, the parties should consult with individuals that possess sufficient technical knowledge and experience regarding ESI.

Principle 2 (Meet and Confer)

As soon as possible after arraignment, the parties must meet and confer to determine whether there are issues in the case associated with the production of ESI. During the meet and confer,

¹ These principles and recommendations are based on and drawn from *Criminal e-Discovery, A Pocket Guide for Judges*, published in 2015 by the Federal Judicial Center. A copy of this publication may be accessed online at: [http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/\\$file/Criminal-e-Discovery.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/$file/Criminal-e-Discovery.pdf).

² These principles and recommendations 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 a criminal or civil investigation. The legal principles, standards, and practices applicable to the discovery phase of criminal cases serve different purposes than those applicable during the investigative phase of a criminal or civil matter. These principles and recommendations also do not alter the parties' discovery obligations or protections under the United States Constitution, the Federal Rules of Criminal Procedure, the Jencks Act, or other federal statutes, case law, or local rules. They may not serve as the basis for allegations of misconduct or claims for relief and they do not create any rights or privileges for any party.

³ *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases*, (ESI Protocol), Joint Working Group on Technology in the Criminal Justice System (JETWG), February 2012, page 4. A copy of the ESI Protocol may be accessed online at: <https://www.fd.org/docs/litigation-support/final-esi-protocol.pdf>

the court encourages the parties to use the Discovery of ESI Production Checklist (attached as Appendix B). The parties should address issues such as the nature, volume, and mechanics of producing ESI in the case. In order for the parties to notify the Court of ESI production issues or problems that they reasonably anticipate will significantly affect the handling and scheduling of the case, the meet and confer must occur prior to the time the Court is asked to rule on a motion to continue the case off the initial trial docket setting. The parties should address other issues they can reasonably anticipate, such as protective orders, “claw-back” agreements between the Government and criminal defendant(s), or any other issues associated with the preservation or collection of ESI. Where the e-discovery is particularly complex, voluminous, or produced on a rolling basis, the parties must maintain an on-going dialogue regarding the schedule for producing discovery.

Principle 3 (Production Format)

The 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. Because the volume of e-discovery frequently requires the use of software tools for discovery review, ESI must be produced in a manner that permits electronic search, retrieval, sorting, and management. If the producing party has not created a table of contents prior to commencing e-discovery production, it should consider creating one describing the general categories of information available as e-discovery. A table of contents is intended to be a general, high-level guide to the categories of ESI. Because a table of contents may not be detailed, complete, or free from errors, the parties still have the responsibility to review the e-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 nothing more than a folder structure where like items are placed into folders for that type of item.

Principle 4 (Transmitting Discovery)

The method and media for transmitting e-discovery should promote efficiency, security, and reduced costs. The party producing discovery should provide a general description of what was transmitted and maintain a record of what was transmitted.

Principle 5 (Production Costs)

The party producing e-discovery is not 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.

Principle 6 (Multi-Defendant Cases)

In cases with multiple defendants and/or where the ESI production is particularly complex, voluminous, or produced on a rolling basis, the defendants should authorize one defense counsel

to act as the discovery coordinator for all the defendants or seek appointment of a Coordinating Discovery Attorney.

Principle 7 (Dispute Resolution)

The parties must make good-faith efforts to discuss and resolve disputes over e-discovery. Before filing any e-discovery motion or any motion alleging e-discovery misconduct, abuse, or neglect, counsel for the moving party must have, in good faith, conferred or attempted to confer by telephone or in person with opposing counsel concerning the matter. Writing a demand letter is generally not sufficient. When necessary, a party must involve in the discussion those with the requisite technical knowledge and/or seek supervisory approval or authorization.

Principle 8 (Court Notification)

If the e-discovery issue remains unresolved, the moving party may file a discovery motion. The motion must include a statement from counsel for the moving party indicating compliance with the meet-and-confer requirement, explaining why the parties were unable to resolve the dispute, and detailing why court intervention is necessary.

Principle 9 (Dissemination and Disclosure)

All parties must limit dissemination of ESI to members of their litigation team who need and are approved for access and must take reasonable and appropriate measures to secure ESI against unauthorized access or disclosure.⁴

⁴ The Court adopts these principles and recommendations in recognition of the fact that we live in a time where more and more information is being created and stored electronically. Because the February 2012 [ESI Protocol](#) was produced by a working group with representatives from both the criminal defense bar and federal prosecutors, the 2015 Federal Judicial Center's publication, *Criminal e-Discovery, A Pocket Guide for Judges*, refers to the [ESI Protocol](#) as the "practitioner's guide to criminal e-discovery." While the above principles and recommendations adopted by this Court are liberally adapted from the ESI Protocol, the court recognizes and acknowledges that the ESI Protocol contains much more detailed strategies, commentary, and recommendations for ESI discovery production in criminal cases. The Court strongly encourages practitioners to rely on the ESI Protocol as a definitive resource for understanding and analyzing ESI issues in federal criminal cases. As stated in the ESI Protocol, it sets 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." As the electronic information age continues to grow and evolve, the Court will continue to adapt with the development of future principles and recommendations designed to serve this goal.

APPENDIX A

TECHNOLOGY

- PC or Mac computer, including a DVD/CD writer¹
- Printer
- Scanner with ability to convert paper documents to PDF/A format
- Speakers
- Secure internet connection (high speed preferred)
- A web browser such as Windows Internet Explorer²
- Multi-media player such as Windows Media Player
- Word processing program (Microsoft Word highly preferred)
- Presentation, database, and spreadsheet software – similar to what is available in the Microsoft Office Suite
- A PDF program with writing and reading capability, plus the ability to create searchable PDF documents
- An individual e-mail address for the attorney that is private
- Anti-virus software, and attorneys should configure their operating system to automatically run security updates
- The hardware and software to utilize external hard drives and thumb drives³

¹ Regardless of whether counsel uses Apple or Windows based computers, their computer hardware should still support the minimum requirements for currently supported releases of the Windows operating system and Microsoft Office applications, since some litigation support programs will not work with or on Apple operating systems. Alternatively, counsel who primarily rely on or use Apple based computers should have access to a computer that uses a Windows operating system.

² For future upgrades of the CM/ECF system, the Administrative Office of the U.S. Courts urges courts to support the Internet Explorer and Firefox browsers. Firefox updates their browser platform frequently. As a result, CM/ECF functionality will be better supported using the Internet Explorer browser.

³ Attorneys should anticipate the need to upgrade their computer and peripheral equipment a minimum of every five years. Upgrade decisions should be based on what hardware and software will provide the best functionality and compatibility with future versions of CM/ECF.

APPENDIX B

DISCOVERY OF ESI PRODUCTION CHECKLIST¹

- 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 e-discovery 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/electronically
 - Other information
- Have the parties addressed e-discovery 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?
 - Confidential, personal, grand jury, classified, tax return, trade secret, or similar information?
 - Whether email transmission is inappropriate for any categories of ESI?
 - Incarcerated defendant's access to discovery materials?
 - E-discovery volume for receiving party's planning purposes?
 - Parties' software or hardware limitations?
 - Production of ESI from third party digital devices?
 - Forensic images of ESI digital devices?

¹ This checklist is reproduced from the February 2012 [ESI Protocol](#).

- Metadata in third 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, e.g., encryption?
 - Adequate security measures to protect sensitive ESI against unauthorized access or disclosure?
 - Need for protective orders, claw back 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?