Litigation Support Tools Workshop

Presented by
The National Litigation Support Team, Defender Services Office
and
The FPD Offices of the Western District of Missouri and the District of Kansas
March 9, 2018
I. ESI in Federal Criminal Cases
   a. Common Litigation Support Terms
   c. ESI Protocol

II. Organizing and Managing Federal Criminal Discovery
   a. Case Management and Discovery Protocol
   c. Discovery Production Log

III. Requesting Criminal Discovery
   a. Initial Discovery Assessment Checklist
   b. Cellebrite Reader Request Language

IV. Systemic Approaches to Managing Federal Criminal Discovery
   a. Pretrial Conference Guidelines
      i. ND California
      ii. ND Illinois
      iii. Massachusetts
      iv. Nevada
      v. New Jersey
      vi. N Marina Islands
      vii. WD Oklahoma
      viii. Puerto Rico
      ix. ND West Virginia
b. Excerpt from 2017-18 Rules Committee of the U.S. Judicial Conference

c. Sample Complex Case Management Order (CD California)

V. dtSearch Information
   a. Quick Start

VI. Adobe Acrobat Pro
   a. Acrobat Best Deals
   b. Acrobat: Find and Advanced Search Tools
   c. Acrobat Pro Document Unitization

VII. Obtaining Resources for the Management of Federal Criminal Discovery
   a. Availability of Casepoint Online Document Review Platform
   b. Availability of Box.com Services
   c. Availability of dtSearch Desktop Software
   d. Litigation Support Strategies
      i. Web Resources
      ii. Criminal ESI Protocol; [www.fd.org](http://www.fd.org)
      iii. Selected Litigation Support Tools
   e. CJA Technology Resources
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annotation</td>
<td>The changes or additions made to a document using sticky notes, a highlighter, or other electronic tools.</td>
</tr>
<tr>
<td>Attachment</td>
<td>A memorandum, letter, spreadsheet, or any other electronic document appended to another document or email.</td>
</tr>
<tr>
<td>Boolean search</td>
<td>Boolean Searches use the logical operators “and”, “or” and “not” to include or exclude terms from a search.</td>
</tr>
<tr>
<td>Chain of evidence</td>
<td>The &quot;sequencing&quot; of the chain of evidence follows this order: identification and collection; analysis; storage; preservation; transportation; presentation in court; return to owner.</td>
</tr>
<tr>
<td>Concept search</td>
<td>Maps relationships between each word and every other word in large sets of documents and then associates words based on the context in which they are used. Two techniques can be used to perform concept searches: the use of a manually constructed thesaurus which relates certain words to others or semantic indexing, a fully automated methods to show associations among words based, in part, on statistical analysis of the occurrence of proximity of certain words to others.</td>
</tr>
<tr>
<td>De-duplication</td>
<td>The process of identifying (and/or removing) additional copies of identical documents in a document collection.</td>
</tr>
<tr>
<td>Discovery</td>
<td>The disclosure of facts, documents, electronically stored information and tangible objects by an adverse party.</td>
</tr>
<tr>
<td>Electronic document</td>
<td>A document that has been scanned, or was originally created on a computer.</td>
</tr>
<tr>
<td>Electronically Stored Information (ESI)</td>
<td>Any information created, stored, or best utilized with computer technology of any type. It includes but is not limited to data; word-processing documents; spreadsheets; presentation documents; graphics; animations; images; e-mail and instant messages (including attachments); audio, video, and audiovisual recordings; voicemail stored on databases; networks; computers and computer systems; servers; archives; backup or disaster recovery systems; discs, CDs, diskettes, drives, tapes, cartridges and other storage media; printers; the Internet; personal digital assistants; handheld wireless devices; cellular telephones; pagers; fax machines; and voicemail systems.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The coding of messages to increase security and make transmission only readable by recipients with the ability to decode only by using the same algorithms.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Forensics</td>
<td>For electronic data, the discovery discipline that includes the physical acquisition of digital data using a methodology that satisfies evidentiary requirements of chain-of-custody and authentication. Forensics can include preserving the evidence, performing code and encryption cracking, searching and retrieving elusive data, determining if files have or have not been deleted, recovering deleted files, and determining use, including Internet, network access, printing, filing, and copying.</td>
</tr>
<tr>
<td>Full text search</td>
<td>Every word in the ESI is indexed into a master word list with pointers to the location within the ESI where each occurrence of the word appears.</td>
</tr>
<tr>
<td>Fuzzy search</td>
<td>Subjective content searching (as compared to word searching of objective data). Fuzzy Searching lets the user find documents where word matching does not have to be exact, even if the words searched are misspelled due to optical character recognition (OCR) errors. This search locates all occurrences of the search term, as well as words that are “close” in spelling to the search term.</td>
</tr>
<tr>
<td>Hash</td>
<td>An algorithm that creates a value to verify duplicate electronic documents. A hash mark serves as a digital thumbprint.</td>
</tr>
<tr>
<td>Index</td>
<td>The searchable catalog of documents created by search engine software. Also called “catalog.” Index is often used as a synonym for search engine.</td>
</tr>
<tr>
<td>Keyword search</td>
<td>A search for documents containing one or more words that are specified by a user.</td>
</tr>
<tr>
<td>Load file</td>
<td>A file that relates to a set of scanned images or electronically processed files, and indicates where individual pages or files belong together as documents, to include attachments, and where each document begins and ends. A load file may also contain data relevant to the individual documents, such as metadata, coded data, text, and the like. Load files must be obtained and provided in prearranged formats to ensure transfer of accurate and usable images and data.</td>
</tr>
<tr>
<td>Logical unitization</td>
<td>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.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>An area on a storage device where email is placed. In email systems, each user has a private mailbox. When the server receives email, the mail system automatically puts it in the appropriate mailbox.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Metadata</td>
<td>Data typically stored electronically that describes characteristics of ESI, found in different places in different forms. Can be supplied by applications, users or the file system. Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image.</td>
</tr>
<tr>
<td>Mirror image</td>
<td>Used in computer forensic investigations and some electronic discovery investigations, a mirror image is a bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination. May also be referred to as “disc mirroring,” or as a “forensic copy.”</td>
</tr>
<tr>
<td>Native application</td>
<td>Any application used to create and view a particular application file type.</td>
</tr>
<tr>
<td>Native format</td>
<td>Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the “native format” of the document. Because viewing or searching documents in the native format may require the original application (for example, viewing a MicrosoftWord document may require the MicrosoftWord application), documents may be converted to a neutral format as part of the record acquisition or archive process. “Static” formats (often called “imaged formats”), such as TIFF or PDF, are designed to retain an image of the document as it would look viewed in the original creating application but do not allow metadata to be viewed or the document information to be manipulated. In the conversion to static format, the metadata can be processed, preserved and electronically associated with the static format file. However, with technology advancements, tools and applications are becoming increasingly available to allow viewing and searching of documents in their native format, while still preserving all metadata.</td>
</tr>
<tr>
<td>Nesting</td>
<td>Document nesting occurs when one document is inserted within another document (i.e., an attachment is nested within an email; graphics files are nested within a Microsoft Word document).</td>
</tr>
<tr>
<td>Objective coding</td>
<td>Extracting information from electronic documents such as date created, author, recipient, CC, and linking each image to the information in pre-defined objective fields. In direct opposition to subjective coding where legal interpretations of data are linked to individual documents.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>Optical Character Recognition (OCR)</td>
<td>A technology process that translates and converts printed matter on an image into a format that a computer can manipulate (ASCII codes, for example) and, therefore, renders that matter text searchable. OCR software evaluates scanned data for shapes it recognizes as letters or numerals. All OCR systems include an optical scanner for reading text, and software for analyzing images. Most OCR systems use a combination of hardware (specialized circuit boards) and software to recognize characters, although some inexpensive systems operate entirely through software. Advanced OCR systems can read text in a large variety of fonts, but still have difficulty with handwritten text. OCR technology relies upon the quality of the imaged material, the conversion accuracy of the software, and the quality control process of the provider. The process is generally acknowledged to be between 80 and 99 percent accurate.</td>
</tr>
<tr>
<td>Physical unitization</td>
<td>Physical unitization utilizes actual objects such as staples, paper clips and folders to determine pages that belong together as documents for archival and retrieval purposes.</td>
</tr>
<tr>
<td>Proximity search</td>
<td>Retrieves a word only when it occurs within a specific number of lines or words of another word.</td>
</tr>
<tr>
<td>Redact</td>
<td>A portion of an image or document is intentionally concealed to prevent disclosure of specific portions. Often done to conceal and protect privileged portions or avoid production of irrelevant portions that may contain highly confidential, sensitive or proprietary information.</td>
</tr>
<tr>
<td>Spoliation</td>
<td>Spoliation is the destruction or alteration of evidence during on-going litigation or during an investigation or when either might occur sometime in the future. Failure to preserve data that may become evidence is also spoliation.</td>
</tr>
<tr>
<td>Subjective coding</td>
<td>The coding of a document using legal interpretation as the data that fills a field. Usually performed by paralegals or other trained legal personnel.</td>
</tr>
<tr>
<td>Tagged Image File Format (TIFF)</td>
<td>Graphic files that portray a single page of a file for viewing purposes with a .tif extension (in the case of Multi-page TIFFs, output images can consist of multiple pages).</td>
</tr>
<tr>
<td>Unicode</td>
<td>Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language (using more than one byte to represent each character, Unicode enables most written languages in the world to be represented using a single character set).</td>
</tr>
</tbody>
</table>
Criminal E-Discovery
A Pocket Guide for Judges

Sean Broderick
National Litigation Support Administrator
Administrative Office of the U.S. Courts, Defender Services Office

Donna Lee Elm
Federal Defender
Middle District of Florida

Andrew Goldsmith
Associate Deputy Attorney General & National Criminal Discovery Coordinator
U.S. Department of Justice

John Haried
Co-Chair, eDiscovery Working Group — EOUSA
U.S. Department of Justice

Kiran Raj
Senior Counsel to the Deputy Attorney General
U.S. Department of Justice

Federal Judicial Center
2015

This Federal Judicial Center publication was undertaken in furtherance of the Center’s statutory mission to develop educational materials for the judicial branch. While the Center regards the content as responsible and valuable, it does not reflect policy or recommendations of the Board of the Federal Judicial Center.
second printing
# Table of Contents

I. Overview ................................................................. 1  
   A. Lack of Criminal e-Discovery Guidance .................. 1  
   B. Civil e-Discovery Rules and Practices Do Not Lend  
      Themselves to Criminal e-Discovery ..................... 2  
   C. A Practitioner’s Guide to Criminal e-Discovery ...... 4  

II. Common Issues in Criminal e-Discovery ................. 5  
   A. Funding the Defendant’s e-Discovery .................... 5  
   B. Lack of ESI Experience, Knowledge, and Competency  
      10  
   C. Necessity of Litigation Support Assistance ........... 11  
   D. The Workflow in Processing ESI ......................... 12  
   E. Varieties of Evidence-Review Software ................ 13  
   F. Volume of e-Discovery ...................................... 13  
   G. Form of Production — ESI Formats ..................... 14  
   H. Form of Production — Paper Formats .................. 16  
   I. Disorganized and Redundant ESI ............................ 17  
   J. Providing Incarcerated Defendants Access to e-Discovery 17  
   K. Multiple Defendants ....................................... 18  

III. Judicial Management of Criminal e-Discovery .... 19  
   A. Managing Voluminous e-Discovery in Criminal Cases 19  
   B. Early Discussion of e-Discovery Issues .................. 20  
      Ask About the Case ........................................ 21  
      Advise About Expectations ............................... 21  
      Advise About Resources ................................ 22  
      Schedule Discovery Conferences ....................... 22  
   C. Subsequent Status of e-Discovery Issues ............. 22  

IV. Conclusion ........................................................... 23  

Appendix A: ESI Protocol Description ....................... 25  
Appendix B: ESI Protocol ............................................ 35  
Appendix C: First Appearance e-Discovery Colloquy .... 73  
Appendix D: Discovery Status Conference e-Discovery  
Colloquy .......................................................... 81
I. Overview

The rapid growth of digital technology and its spread into every facet of life are producing increasingly complex discovery issues in federal criminal cases. There are several advantages to electronically stored information (ESI, or e-discovery), including speed, efficiency, and quality of information. To ensure these benefits are realized, judges and lawyers working on federal criminal cases need guidance on how best to address e-discovery issues.

Judges can play a vital oversight role to ensure that e-discovery moves smoothly, trial deadlines are met, and the parties and courts are able to review and identify critical evidence. This pocket guide was developed to help judges manage complex e-discovery in criminal cases. A note of appreciation goes to Judge Xavier Rodriguez (W.D. Tex.), and Magistrate Judges Laurel Beeler (N.D. Cal.) and Jonathan W. Feldman (W.D.N.Y.), for their suggestions and advice, as well as to our fellow members of the Joint Electronic Technology Working Group, who improved this publication.

A. Lack of Criminal e-Discovery Guidance

Although the Federal Rules of Criminal Procedure offer guidance on a number of topics, they offer little help to judges and litigants concerning how to conduct e-discovery. As the Sixth Circuit noted in United States v. Warshak, Rule 16 of the Federal Rules of Criminal Procedure is “entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed.”1 To be sure, Rule 16 provides a court the discretion to fashion discovery orders to serve the particular needs of a case, but it does not “specify the manner in which production is done.”2

---

1. 631 F.3d 266, 296 (6th Cir. 2010). In that case, the defendant argued that the “district court must order the government to produce electronic discovery in a particular fashion.” In rejecting this argument, the court noted that there is “a dearth of precedent suggesting that the district court was wrong” in allowing the government to produce discovery in an electronic format different from what the defendant sought. Id.

Criminal e-Discovery

B. Civil e-Discovery Rules and Practices Do Not Lend Themselves to Criminal e-Discovery

The rules governing civil and criminal discovery are fundamentally dissimilar due to the different public policies underlying criminal and civil litigation, constitutional requirements, and special ethical obligations of prosecutors and defense counsel. Consequently, courts have generally refrained from applying civil e-discovery rules to criminal discovery.3

An essential difference between civil and criminal discovery is breadth:

A criminal defendant is entitled to rather limited discovery, with no general right to obtain the statements of the Government’s witnesses before they have testified. Fed. Rules Crim. Proc. 16(a)(2), 26.2. In a civil case, by contrast, a party is entitled as a general matter to discovery of any information sought if it appears “reasonably calculated to lead to the discovery of admissible evidence.” Fed. Rule Civ. Proc. 26(b)(1).4

Federal Rule of Criminal Procedure 16 does not mandate any mechanisms or procedures for addressing e-discovery equivalent to those found in Federal Rules of Civil Procedure 26 and 34. Rule 16 includes “data” as a proper object of criminal discovery, but the rule does not address the mechanics of e-discovery.

Furthermore, the nature of the parties and proceedings differ in criminal cases. Unlike civil cases, where discovery is an adversarial process in which the government’s discovery obligations are similar to any litigant’s, the government has unique nonadversarial discovery obligations in criminal cases. As a representative of the sovereign, prosecutors are obliged to prosecute impartially and ensure that justice

I. Overview

is done.\textsuperscript{5} For example, the Due Process Clause imposes a “fundamental fairness” requirement on the government’s discovery, as expressed in the government’s \textit{Brady} and \textit{Giglio} obligations.\textsuperscript{6} Additionally, speedy trial rights may be implicated when defendants have little time to come to grips with vast e-discovery.\textsuperscript{7} Similarly, defendants are entitled to effective assistance of counsel at trial and during plea negotiations.\textsuperscript{8} Defense counsel’s effectiveness may depend on whether he or she has reviewed and understands the e-discovery in time to enter into informed plea negotiations.\textsuperscript{9} When the government provides e-discovery in a reasonably organized fashion, it can help the defense efficiently review discovery and can lead to more productive plea discussions, less litigation, and speedier resolution of a case.

Criminal investigations and third-party subpoenas by both the prosecution and defense often bring vast quantities of ESI to criminal e-discovery. Complex ESI cases usually require litigation support resources not typically found in criminal defense practices. Indigent defendants need adequate funding to obtain those resources.

\textsuperscript{5} ABA Model Rules of Professional Responsibility 3.8, comm. 1; see also Berger v. United States, 295 U.S. 78 (1935).

\textsuperscript{6} See also United States v. Bagley, 473 U.S. 667, 675 (1985) (withholding \textit{Brady} evidence violates due process). The prosecutor’s \textit{Brady} obligation is addressed in ABA Model Rule of Professional Conduct 3.8(d) (requiring prosecutors to “make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and, in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal.”).

\textsuperscript{7} See U.S. Const. amend. VI; 18 U.S.C. § 3161 (“Speedy Trial Act”).


\textsuperscript{9} Although lawyers need not review every document in a voluminous e-discovery production before entering into a plea bargain, they should review a reasonable and targeted portion of discovery so as to provide reasonably effective advice regarding resolution. Thus, depending upon the nature and complexity of the e-discovery, to conduct plea negotiations the defense may need to have e-discovery in a reasonably useable format, and have engaged in thoughtful e-discovery review.
Criminal e-Discovery

C. A Practitioner’s Guide to Criminal e-Discovery

One attempt to provide comprehensive, national guidance is the ESI Protocol (see Appendices A & B), which was produced by a joint working group composed of the Department of Justice and representatives of the criminal defense bar. The ESI Protocol is one approach for judges to use to encourage interparty cooperation and reduce the need for judicial intervention. Indeed, some federal district courts have begun integrating the ESI Protocol into their courtroom practices.

The ESI Protocol draws on many sources, including case law, local rules, and seasoned defense and prosecution practitioners’ experience. Its goal is to provide courts and litigants with best practices consisting of general principles, recommendations, and concrete strategies for improving efficiency, minimizing expense, increasing security, and decreasing frustration and litigation. Importantly, the ESI Protocol does not enlarge or diminish any party’s substantive legal discovery obligations imposed by applicable federal statutes, rules, or case law.

---

10. The Recommendations for Electronically Stored Information Discovery Production in Federal Criminal Cases (hereinafter “the ESI Protocol”) was produced by the Joint Electronic Technology Working Group (JETWG), which comprises representatives of the Administrative Office of the U.S. Courts (AOUSC), Defender Services Office (DSO), the Department of Justice (DOJ), Federal Public and Community Defender Organizations (FPDOs and CDOs), private attorneys who accept Criminal Justice Act (CJA) appointments, and liaisons from the United States Judiciary and other AOUSC offices. The Federal Judicial Center does not endorse any specific discovery approach, including the ESI Protocol.


II. Common Issues in Criminal e-Discovery

The ESI Protocol will be familiar to most federal criminal practitioners. The Department of Justice trains its prosecutors to use the ESI Protocol in cases involving complex e-discovery. Most federal defenders and Criminal Justice Act (CJA) representatives receive similar training on the ESI Protocol.

II. Common Issues in Criminal e-Discovery

Both prosecutors and defense attorneys struggle with the same e-discovery issues: large volume; a variety of sources and formats; hidden information (metadata and embedded data); differing formats for production; software and hardware limitations; and finding efficient, cost-effective ways to review ESI. Some challenges are unique to criminal practice, such as incarcerated defendants’ access to e-discovery, while others are the same as those arising in civil practice. For many prosecutors and defense counsel, a lack of experience with ESI presents a significant challenge; but it is the lack of resources—money, personnel, training—that often overshadows all other problems. And even when resources are available, considerable time is often required to arrange for and execute the processing necessary to make ESI readily available.

For CJA counsel, the challenges of ESI may be especially daunting. Often, they are solo practitioners who lack the resources for sophisticated software tools. Because they are usually appointed post-indictment, they need to get up to speed on matters that the government may have spent many months or years investigating and preparing—while at the same time getting up to speed on how to manage electronic discovery. Besides training and software tools, they often may need experienced litigation support assistance, which can be provided pursuant to 18 U.S.C. § 3006A.

The following are e-discovery issues that judges may need to understand or address.

A. Funding the Defendant’s e-Discovery

There was a time when voluminous e-discovery cases were confined to white-collar prosecutions, and those defendants typically paid the costs
of their own defense. Today, even routine drug cases and bank robberies often involve extensive cell phone data or other ESI.\textsuperscript{13} This has funding consequences for indigent defendants and the court.

When a case has complex e-discovery issues, the judge considering a CJA appointment may need to factor in the additional cost of reviewing, organizing, and working with e-discovery.\textsuperscript{14} The Act is silent about when a defendant would be so destitute as to need appointed counsel, but the cost of working with complex e-discovery can itself exceed what many defendants can afford even if they are able to pay for counsel.\textsuperscript{15}

Some CJA panels have formal tiers or informal lists of specialized lawyers for capital, financial, or immigration cases. Courts that take their CJA attorneys’ skills into consideration can also consider creating

\begin{quote}
\textit{Criminal e-Discovery}
\end{quote}

\textsuperscript{13} Smartphone data provides an example of the magnitude of e-discovery. Many smartphones hold sixteen to sixty-four gigabytes of data, not including storage cards (which can double that amount), and have cloud access to much more data. They contain emails, call history and contact information, calendars, text messages, GPS data, photographs, videos, internet history, and social media information, all of which can result in thousands of potentially relevant items of discovery. Multiple-defendant cases could dramatically increase that amount. Add to that the corresponding laptops, tablets, desktops, and surveillance data also readily accessible, and the amount of e-discovery can quickly exceed document-based paper discovery in a white-collar or corporate prosecution from fifteen years ago.

\textsuperscript{14} The court can ask the government to give it early notice if the case involves voluminous e-discovery.


If counsel anticipates that the costs will exceed the statutory maximum, advance approval should be obtained from the court and the chief judge of the circuit (or the active or senior circuit judge who has been delegated authority to approve excess compensation). See Vol. VII, § 310.20.20 for further information and a sample order, available at http://www.uscourts.gov/rules-policies/judiciary-policies/cja-guidelines/chapter-3-ss-310-general#a310_20.
II. Common Issues in Criminal e-Discovery

a list of those lawyers who are proficient in e-discovery. Although attorneys who lack familiarity with ESI will face a learning curve, experience with cases involving large amounts of ESI over time will develop a set of CJA lawyers readily capable of handling these cases.

In multidefendant cases, the court may be able to minimize costs by calling for cooperative sharing among defendants. This has been done for years whenever there is voluminous paper discovery, and many of those principles can apply to electronic discovery. One of the defense attorneys (often the federal defender) may take the lead for meet-and-confer discussions with the government regarding e-discovery productions and for distributing and providing basic organization of ESI when the defendants enter an agreement concerning discovery. The court can encourage centralizing e-discovery management and can approve a litigation support specialist, a technologist, or a paralegal working under that lawyer’s supervision.

It also may be beneficial to place the discovery into a cloud-based document-review platform, so defendants, counsel, investigators, and experts can access it as needed from various locations. Depending on what software different CJA lawyers have, all co-defendants may not be able to use or take advantage of the same format of ESI production. But any decision to rely on cloud-computing or reviewing services should include consideration of whether that service provider has provided adequate security to protect confidential, privileged, or oth-

16. On the other hand, courts must decide whether to expect all panel members to be prepared to handle e-discovery on a large scale, given that every practitioner should develop a baseline comfort with e-discovery. In August 2012, the ABA modified its ethics rule on competency to include familiarity with technology that may be used in representation. Comment 8 to Model Rule 1.1 provides: “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . .” (emphasis added).

17. A document-review platform uses a database and tools to capture, organize, analyze, and review e-discovery. Whether stand-alone, networked, or in the cloud, these platforms may enable multiple individuals to securely manage and access a large amount of data.

18. By way of example—and not as an endorsement of either Apple computer systems or Microsoft Windows—one common challenge is that a number of CJA-panel attorneys use Apple operating system (“Mac”) computers, but Apple systems work differently than the Windows computers that are standard with the DOJ and FDOs.
Criminal e-Discovery

otherwise sensitive e-discovery.\textsuperscript{19} The Department of Justice and the defense bar expect to address criminal e-discovery security best practices in the near future, but in the interim, counsel should remain vigilant in protecting e-discovery.

Processing “raw” ESI into usable evidence that can be reviewed electronically is expensive and time-consuming.\textsuperscript{20} As of 2015, in a relatively small case, processing five boxes (12,500 sheets) of paper business records costs approximately $4,800 and takes a trained DOJ litigation support professional employee three days. Similarly, processing twenty-five gigabytes of complex ESI costs approximately $3,200 and takes an employee two weeks.\textsuperscript{21} Today, there is no software tool for producing all discovery in a single, easy-to-use package. Hopefully that will change as electronic discovery matures.

Fortunately, there are resources that can provide advice and guidance to judges about cost-effective means of managing e-discovery:

- The National Litigation Support Team (NLST), part of the Defender Services Office (DSO) of the Administrative Office of the U.S. Courts, is available to help attorneys for indigent defendants struggling with extensive e-discovery. The NLST writes recommendations for funding requests, advises courts and parties about economical and practical solutions to e-discovery issues, and provides direct assistance to lawyers.\textsuperscript{22}

\textsuperscript{19} ESI protocol, Recommendation ¶ 10.

\textsuperscript{20} The term “processing” usually involves formatting ESI so that the native file can be placed into a review platform where it can be viewed, culled, organized, searched, and analyzed. For example, processing a native email container file (a collection of emails) involves extracting individual emails and their attachments, while keeping track of the relationship between the emails and attachments, and converting the files to formats that can be read through a review tool. For more information about processing raw ESI see infra section II.D.

\textsuperscript{21} The 2015 market rates for processing ESI range from $125 to $150 per gigabyte.

\textsuperscript{22} Before seeking court approval for any computer hardware or software with a cost exceeding $800, or for utilizing computer systems, litigation support products, services, or experts exceeding $10,000, appointed counsel must consult with the DSO for guidance. CJA counsel must then inform the court in writing of the DSO’s advice and recommendation regarding proposed expenditures. Guide to Judiciary Policies and Procedures, vol. VII, § 320.70.40, available at http://www.uscourts.gov/
II. Common Issues in Criminal e-Discovery

The court can ask for assistance from the NLST.23

• The DSO has three national coordinating discovery attorneys (CDAs) who are experts in e-discovery, have experience with CJA cases, and are knowledgeable about litigation technology. They work with CJA counsel and federal defenders in multidefendant cases to manage large volumes of e-discovery efficiently and cost-effectively to best fit the defendants’ needs. The court can ask CJA counsel to request that the case be referred to a CDA through the National Litigation Support Team.24

• All circuits except the Fifth, Eleventh, and D.C. have case budgeting attorneys (CBAs) who work with judges and CJA panel attorneys to develop and review budgets for criminal “mega cases.”25 They assist in addressing attorney and paralegal time, as well as expert, investigative, and other costs, to ensure that critical defense needs are budgeted to optimize resources while fostering high-quality, cost-controlled represen-

---

23. The NLST can be contacted at (510) 637-3500. Further information about the NLST can be found on fd.org at http://www.fd.org/navigation/litigation-support/subsections/who-is-the-national-litigation-support-team.


25. For CJA panel attorneys, “mega cases” are either: (a) federal capital prosecutions and capital habeas corpus cases, or (b) noncapital representations with the potential for extraordinary cost (attorney work expected to exceed 300 hours or total expenditures for attorneys and investigative, expert, and other service providers expected to exceed $30,000 for an individual CJA defendant). This is distinguished from “mega budget cases,” referring to federal and community defender office cases that will substantially impact their office budgets (by a 10% or $500,000 increase or more), so that an additional budget is developed to fund just that one case. See Case-Budgeting Techniques and Other Cost-Containment Policies (June 30, 2014), available at http://www.fd.org/docs/select-topics/cja/case-budgeting-techniques-and-other-cost-containment-strategies.pdf?sfvrsn=8.
Criminal e-Discovery

tation. In appropriate cases, the budgets may address litigation support costs, and the CBAs have working relationships with the NLST to consult on litigation support matters. Judges in a district without a CBA can contact the DSO for assistance.26

There are considerable funding consequences to voluminous e-discovery. The court should expect additional CJA costs in these cases, but managing e-discovery can be done thoughtfully and reasonably to mitigate costs.

B. Lack of ESI Experience, Knowledge, and Competency

Unfortunately, many criminal practitioners still do not have an adequate understanding of e-discovery issues and litigation technology. However, attorney competency ethics standards are evolving to require an adequate understanding of e-discovery and the technology needed to review it.27 Lawyers who are unfamiliar with e-discovery can associate or consult with others who have the expertise.28 Nonetheless, they remain responsible for e-discovery decisions and should be able to do the following, either themselves or in association or consultation with others:

• Implement procedures to preserve potentially discoverable electronic information.

26. Further information on case budgeting and case budgeting attorneys can be found on the J-Net at http://jnet.ao.dcn/court-services/cja-panel-attorneys-and-defenders/case-budgeting (not accessible to public). Judges who do not have a CBA in their circuit can contact the duty attorney for the Defender Services Office at (800) 788-9908.

27. For example, the State Bar of California issued a formal ethics opinion on this subject in the summer of 2015. See State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2015-193 (2015). This development follows the 2012 American Bar Association amendment to its Model Rule 1.1, stating that lawyers need to “keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.” ABA Model Rules of Professional Conduct, Model Rule 1.1, comt. 8 (emphasis added).

28. If a CJA attorney needs to retain expert assistance, payment would have to be approved by the court.
II. Common Issues in Criminal e-Discovery

- Assess e-discovery needs and issues.
- Plan and perform appropriate searches.
- Understand how to manage, review, and produce e-discovery in a manner that preserves its integrity.

Because discoverable information is increasingly found and produced electronically, lawyers who are e-discovery illiterate may delay trial preparation. Technological “dinosaurs” may also miss potentially beneficial evidence, for example, by overlooking valuable metadata in electronic records because they are entrenched in printing their discovery. They also may make critical mistakes early in the case, inadvertently choosing production formats that they cannot use or that will not help find the evidence they need. When such mistakes result in not finding exculpatory evidence, they risk being ineffective.

The benefits of e-discovery can be lost on uninformed counsel. In making counsel appointments and resourcing cases, judges should be mindful that handling complex e-discovery cases requires an adequate understanding of ESI and available technology.

C. Necessity of Litigation Support Assistance

In any sizeable e-discovery case, finding appropriately skilled expert assistance is critical to reviewing the evidence and deciding whether to negotiate a plea agreement or take the case to trial. Individuals with litigation support expertise can be found in a variety of traditional job roles, working as paralegals, investigators, information technology (IT) specialists, computer technicians, data processors, software specialists, and more. Finding the correct fit of litigation support staff to the case early is a priority.

Litigation support specialists should have legal and IT experience and training to organize, analyze, and present case materials through technology equipment and computer programs. They should have the ability to harvest and extract electronic data and metadata from ESI; assist in meet-and-confer sessions regarding the exchange of ESI; monitor and manage discovery productions (both production and receipt); provide advice on how to search data; and manage the day-to-day operations of strategically collecting, processing, organizing, reviewing,
Criminal e-Discovery

analyzing, and presenting case data. Using both project management and technology, they ensure that e-discovery is handled in a cost-effective and time-efficient manner that allows for effective organization, easy retrieval, and quality client representation.

Just as judges should be mindful of attorney knowledge and experience in managing e-discovery, they should also be aware that even knowledgeable attorneys need skilled litigation support.

D. The Workflow in Processing ESI

ESI generally takes one of two possible forms: preprocessed (raw) or postprocessed. Some raw ESI is not ready to be reviewed electronically; it must be processed\textsuperscript{29} into a digital file that can be loaded into document-review software. Similarly, paper records can be processed into electronic files like TIFFs with extracted text or searchable PDFs with the extracted text embedded in the file itself.

The workflow for processing ESI can be complicated. When ESI is in a proprietary format (for example, a Google Mail file), it cannot be reviewed with industry-standard tools; instead, review requires specialized hardware, software, and expertise to convert the data into a form that can be reviewed with standard tools.\textsuperscript{30} Even if the discovery is produced in an optimal way,\textsuperscript{31} defense counsel may still need expert assistance, such as litigation support personnel, paralegals, or database vendors, to convert e-discovery into a format they can use and to decide what processing, software, and expertise is needed to assess the ESI. Next, the ESI should be organized to facilitate finding informa-

\textsuperscript{29} See supra n. 20 for a definition of “processing.”

\textsuperscript{30} Many state and federal law enforcement agencies have outdated computer systems, so the data in these outdated systems cannot be viewed with current industry-standard litigation support software. This is particularly common with audio and video files, necessitating conversion to industry-standard formats.

\textsuperscript{31} Parties should not be obstructionist and ought to produce discovery in a usable format if they reasonably can. According to the ESI Protocol, when a producing party elects to engage in processing ESI, the results of that processing (unless it contains work product) should be produced as discovery; this saves the receiving party the expense of replicating the work. ESI Protocol, Recommendations ¶ 6(d). That said, the ESI Protocol states that the government is not obligated to convert ESI into a format specified by the defense beyond what it would do for its own case preparation or discovery production.
II. Common Issues in Criminal E-Discovery

In voluminous e-discovery cases, parties must be able to rely on document-review software, which can be costly. Nonetheless, it saves money because it speeds up the review process and improves counsel’s ability to find information. Such software affords counsel a variety of search strategies, including word searches, document searches, date searches, sender/recipient searches, concept searches, and predictive coding searches.32

E. Varieties of Evidence-Review Software

There is a vast array of software tools for handling all of the stages of electronic discovery: preserving, collecting, and harvesting data; processing and/or converting ESI; searching and retrieving information; reviewing ESI; and presenting evidence. There is frequently overlap between what various products can do. No single software tool does everything needed for e-discovery. Some tools specialize in processing raw ESI into formats that another tool can then use, while other tools specialize in a discrete function such as document review, strategic analysis, case organization, production of discovery, or evidence display in the courtroom. As a result, litigants have different collections of tools. That creates compatibility and conversion issues.

A meet-and-confer is an important stage in tackling those compatibility and conversion issues, particularly when the parties do not already have an established routine for exchanging discovery or when they face novel or difficult ESI issues. One goal of the meet-and-confer is to address technical issues so that the ESI produced in discovery is readable and usable. An important part of that process is the parties’ discussion of production formats, volume, timing, and other issues.33

F. Volume of E-Discovery

The great volume of e-discovery poses a serious challenge due to the variety of devices on which ESI can be created and stored, the ease of

32. Technology-assisted review (also called predictive coding) is a process for prioritizing or coding a collection of documents using a computerized system that harnesses human judgments of one or more subject matter expert(s) on a smaller set of documents, and then extrapolates those judgments to the remaining data.

33. See ESI Protocol, attached as Appendix B.
Criminal e-Discovery

various forms of telecommunication (such as texting and social media), and the declining cost of storage. ESI can come from many custodians or sources—mobile phones, smartphones, tablets, laptops, desktops, computer network servers, external ESI storage devices (such as flash drives or external hard drives), cloud storage, GPS tracking devices, social media. Because of this, the amount of ESI in criminal cases has grown exponentially, and this growth is expected to continue, significantly complicating management and review of evidence. For example, in 2011, court-appointed defense counsel in one multi-defendant case had to review discovery comprising 240,000 pages of documents on 19 DVDs and CD ROMS, 185 banker boxes of paper documents (approximately 460,000 pages), and 30 forensic images (that is, copies) of complete computers, servers, and thumb drives holding approximately 4.3 terabytes of data. Additionally, the defendants gathered 750,000 pages of third-party information directly relevant to their defenses. Cases like this benefit substantially from sophisticated software and advanced review practices such as technology-assisted review.

It is important to recognize that complex ESI requiring technological assistance is not constrained to computer and white-collar fraud crimes. Vast amounts of ESI are found in small cases as well. Even relatively modest amounts of e-discovery, depending on format, can create obstacles to reviewing evidence. Moreover, simple cases of possession of drugs or guns, for example, can involve smartphones and computers containing gigabytes or even terabytes of data. Lawyers unaided by technology cannot review this much data.

G. Form of Production—ESI Formats

The format in which ESI is gathered affects how the data can be used. For example, text messages collected as text-only files can be searched for particular words or combinations of words. But if the metadata for those same text messages is also gathered, then thousands or millions of text messages can not only be searched for particular words, they

34. In e-discovery terms, “custodian” refers to the person whose data was collected.

35. Applying litigation support standard calculations, 4.3 terabytes of data is the equivalent of 215 million pages, or 86,000 banker boxes, of documents.
II. Common Issues in Criminal e-Discovery

can also be sorted by date, custodian, and author or addressee, and software can plot who communicated with whom, how frequently, when, and where. Such information can have tremendous utility in criminal cases.

Lawyers need specialized litigation software to work with ESI in its many formats. For example, they need software to review ESI documents, which can be as basic as a PDF viewer or far more complex. Most document-review platforms allow parties to view many file types. The DOJ and most civil law firms have managed their own discovery materials with software programs and technical personnel for years. Criminal defense practitioners, especially those involved in indigent defense, are relative latecomers to this world. Most CJA panel attorneys do not have litigation support software that can view and organize TIFF or native file productions. Similarly, most do not have tools to take advantage of a “load file,”36 extracted metadata, or files in native or near-native ESI format.37 It is only recently that federal defender offices gained that capability nationally. As a result, the DOJ may be able to produce discovery in a reasonably usable format, but CJA counsel may not be able to utilize the most robust litigation software available. To provide computer-challenged defense counsel with reasonably usable e-discovery, the U.S. Attorney’s Office typically provides e-discovery on disks that contain software for viewing, searching, and tagging documents. For more sophisticated defense counsel, the DOJ typically creates load files or otherwise configures its e-discovery productions in industry-standard formats. Of course, there are instances where typical practices do not work well, and those are proper subjects for a meet-and-confer.

To benefit from the information available in e-discovery, attorneys must know what format the original data was in, what formatting options are available, and how those options affect their potential review

36. A load file is a cross-reference file used to import images or data into databases. A data load file may contain Bates numbers, metadata, paths 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.

37. A significant advantage to web-hosted document-review platforms for the CJA panel is that IT support is provided by the vendor, since most do not have in-house IT staff.
of the data. Attorneys who do not understand the various formats should consult with a litigation support or IT expert before receiving or processing their e-discovery.

H. Form of Production—Paper Formats

Some contemporary records and many historical records only exist on paper. Converting paper discovery to electronic formats makes it easier to duplicate, exchange, and search. But converting voluminous paper records takes time and money. Accurate document breaks (also known as document unitization\(^{38}\)) too frequently are not captured when scanning paper records. When this happens, document unitization is lost, diminishing the utility of the resulting electronic files. Although the producing party is not obligated to reformat paper records into an electronic form,\(^{39}\) in some cases both parties may save time and money by converting paper into electronic formats. Cost sharing may be an option if the parties agree that scanning serves both sides.

Scanning a paper record and making it searchable through optical character recognition (OCR) software is an improvement over leaving it in paper form, but it is not a perfect solution. Scanning can be prohibitively expensive. Moreover, OCR programs have established error rates, decreasing the accuracy and reliability of electronic searches of documents. That unreliability causes some attorneys to default to using their own eyes to search rather than scanning paper records for electronic review.

Today, some records custodians’ systems still are configured to produce subpoenaed records in paper, even when they have the same data electronically. If a records custodian is willing to produce the information in an electronic format, the electronic version usually will yield more reliable searches.\(^{40}\) However, what is efficient and afforda-

---

38. 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.


40. There are several options for electronic formats. Sometimes the records custodian can produce the native-format version, for example, a Word document as a Word file as opposed to a paper document or a PDF. Sometimes the native format
II. Common Issues in Criminal e-Discovery

ble for records custodians, and what electronic formats they are willing or able to produce, varies widely.

I. Disorganized and Redundant ESI

E-discovery can come from records custodians as a disorganized and redundant jumble. That sometimes arises from how custodians store their data: multiple versions of the same computer record may coexist in unrelated computer systems, especially with cloud computing. Custodians may not be aware that copies of files exist in different parts of their system since files are often copied or backed up automatically without user interaction. With the ease of web communication, the multitude of different mobile devices, and inexpensive storage, ESI is frequently copied, recopied, forwarded, backed up, and archived many times over, resulting in multiple copies of the same files. Unlike paper records, where information was actively managed by records custodians who culled records to save money, there is often little need to organize ESI and delete duplicates or drafts. Although no single software quickly solves the issue of disorganized and redundant ESI, there are workflow processes combined with different types of software that can assist counsel in reducing duplicates, organizing the materials, and identifying the most relevant information more quickly than having a human look at every page.

J. Providing Incarcerated Defendants Access to e-Discovery

Defendants in pretrial detention face significant e-discovery challenges. Their rights to assist in their defense and confront the evidence against them contemplate reviewing that evidence. When out of custody, they can use their own (or their attorney’s) computers to review electronic

is proprietary, and requires a proprietary viewer. Many video recording systems are proprietary. In some instances, a records custodian can produce a “near-native” version. For example, Google Mail (Gmail) is a web-based email system. For production, a Gmail file can be converted to an .msg file format that can be readily viewed. Alternatively, a document can be produced as an electronic TIFF image with extracted text that can be loaded into a database and electronically searched. Or documents can be converted to a searchable Adobe PDF format.
Criminal e-Discovery

discovery. When detained, their access to computers often is very limited. Although jails have long had policies for managing inmates’ paper discovery, most do not have policies allowing inmates to review electronic discovery. Moreover, when the detention facilities do not have computers readily available for inmate evidence review, acceptable equipment and software must be purchased for incarcerated defendants to use. Although defender offices are budgeted for such equipment, CJA attorneys may need the court to fund equipment purchases or rentals.

Providing defendants in-custody access to technology that allows them to review their e-discovery reduces attorney time and costs. When incarcerated defendants cannot review e-discovery on their own time, the attorney or investigator has to bring a laptop or tablet containing the e-discovery to a jail visit and maintain control of the device while allowing the defendant to review the evidence, resulting in many hours of time billed to the CJA appropriations. Additionally, defendants may be able to locate critical evidence much more quickly than defense team members who are unfamiliar with the documentation. By reviewing and discussing evidence early, defendants help their counsel prioritize the investigation and limit the data that must be reviewed. This also creates more meaningful meetings, allowing both counsel and defendant to make timely decisions.

Jails have legitimate security and staffing interests in preventing inmates from having unfettered access to computers. A joint DOJ and defense attorney working group is studying the risks and benefits of allowing inmates access to computers for e-discovery review. They hope to produce practical recommendations. In the interim, consultation between the government, the defense, and the particular facility is most likely to result in an acceptable solution.

K. Multiple Defendants

Multidefendant, high-volume e-discovery cases are fertile ground for generating discovery disputes that require a judge’s attention. For example, fraud cases involving multiple defendants may include millions of pages of documents. Multiple-defendant drug cases tend to have fewer documents, but they typically make up for that with wiretaps, surveillance photos and videos, text messages, GPS data, and social
III. Judicial Management of Criminal e-Discovery

media. These discovery items cannot be readily searched for defendant-specific materials without the use of litigation technology software. Even with software, it can take considerable time to review and analyze such complex and voluminous information.

With so many variables in play, multidefendant prosecutions may develop more conflicts over discovery than single-defendant prosecutions. One attorney may request additional information about the alleged criminal enterprise to receive more context about the case, while another may request different forms of production. Defense counsel may disagree with each other about formats of production, how the evidence is indexed and organized, and what information they are searching for. Prosecutors can find themselves caught in the middle of these competing demands and may not be able, or may not believe it is reasonable or affordable, to agree to varying (and potentially conflicting) defense counsel requests. This situation is ripe for pretrial e-discovery disputes. Judges can encourage the parties to attempt to resolve disputes without resorting to motion practice but may still be called upon to adjudicate competing discovery interests, especially where the government is subject to conflicting requests.

III. Judicial Management of Criminal e-Discovery

A. Managing Voluminous e-Discovery in Criminal Cases

As discussed earlier, voluminous e-discovery cases present difficult challenges for prosecutors and defense counsel. Depending upon the lawyers’ familiarity with e-discovery, the court may need to exercise oversight in such cases. The ESI Protocol addresses the most common e-discovery issues, and the court can direct the parties to the ESI Protocol for guidance. Often, e-discovery disputes are simply the result of the lawyers’ inexperience with e-discovery or their misunderstanding of technical terminology. Knowing that the lawyers are knowledgeable about e-discovery and/or that they have qualified litigation support, IT, or paralegal assistance will be of great assistance to judges managing these cases.
Criminal e-Discovery

One key to success with these cases is addressing e-discovery issues early. Missteps at the outset of the case are costly to unwind or correct, and they waste time and money. To get the parties to address e-discovery issues early, the ESI Protocol recommends three steps:

1. At the outset of the case, the parties should meet and confer about the nature, volume, and mechanics of producing e-discovery.  
2. At the meet-and-confer, the parties should address what is being produced; a table of contents; the forms of production; volume; software and hardware limitations; inspection of seized hardware; and a reasonable schedule for producing e-discovery.
3. The producing party transmits its e-discovery in sufficient time to permit reasonable management and review, and the receiving party should be proactive about testing the accessibility of the ESI when it is received.

Although the Federal Rules of Criminal Procedure do not specify when evidence must be produced, some judges find it useful to have standing orders that direct the parties to come up with a discovery plan when dealing with complex e-discovery matters.

To get the parties started on the right foot, the court may want to address the topic of e-discovery at one of the initial hearings, even before the parties have conducted their first meet-and-confer session. A discovery status conference can be scheduled after the meet-and-confer takes place. Proposed colloquies are offered in Appendices C and D.

B. Early Discussion of e-Discovery Issues

There are four steps courts can take early on in a large e-discovery criminal case. First, the court can ask the parties questions to ascertain what issues they are facing. Second, the court can be clear about its expectations for parties handling voluminous e-discovery. Third, the

41. ESI Protocol, Recommendations ¶ 5.
42. ESI Protocol, Strategies ¶ 5.
43. ESI Protocol, Strategies ¶ 5(o).
III. Judicial Management of Criminal e-Discovery

court can advise the parties of resources available to assist them. Finally, the court can schedule a discovery status conference as needed.

Ask About the Case: Appendix C offers a sample colloquy for the first appearance in the case. The court can ask the government the threshold question of whether this is a case in which the volume and/or nature of the e-discovery significantly increases the complexity of the case. In cases with court-appointed counsel, the answer may help the court decide whom to appoint and what resources and assistance appointed counsel may need. Once both parties appear, the court can ask whether the parties have already addressed e-discovery issues, as that may obviate the need for further court involvement. The court can further ask if the parties are familiar with the ESI Protocol; if not, the prosecutor can provide a copy to defense counsel.

Advise About Expectations: Given the varying levels of experience and comfort with e-discovery and technology, as well as the rapid evolution of litigation software, the court can make clear from the outset its expectations for the lawyers in a complex e-discovery case.

Appendix C sets forth a list of reasonable expectations for the lawyers. These include the following:

• The lawyers should have an adequate understanding of e-discovery such that they can identify, communicate on, and solve common e-discovery problems and determine what forms of production are possible, how different software products and services can assist in the particular case, and what costs and cost savings result from their choices. The lawyers should be sufficiently familiar with the capabilities and limitations of software and services in order to select appropriate software and outside assistance. Lawyers can, of course, rely on experts to consult and advise them on what programs to use and what staff to retain.

44. See section II.A, supra, regarding funding electronic discovery.
Criminal e-Discovery

- Although the court will encourage parties to obtain technical assistance, the lawyers are ultimately responsible for decisions involving e-discovery.

- The parties will meet and confer once they have secured expert assistance. A meet-and-confer discussion should occur well before any discovery status conference. When appropriate, the lawyers should bring experts with them to the meet-and-confer to address the technical aspects of e-discovery.

Advise About Resources: Public defenders and CJA counsel in multidefendant, complex e-discovery cases can petition the court to appoint a coordinating discovery attorney. If the court appointed counsel (either an assistant federal defender or a CJA panel attorney), counsel can contact the NLST for assistance.  

Schedule Discovery Conferences: Complex e-discovery cases may benefit from one or more discovery conferences, as the court deems appropriate.

C. Subsequent Status of e-Discovery Issues

Appendix D has a proposed colloquy for discovery status conferences. If status conferences are held, the judge can check on the progress of e-discovery. Depending on what the parties report has transpired since the last proceeding, the judge may remind them of the court’s expectations as well as remind them of the resources available to them. Additionally, particular issues may arise that should be addressed in-depth.

Despite strong encouragement from the bench and the best intentions of the parties, the lawyers may not have conducted a meaningful meet-and-confer session. The Seventh Circuit’s civil e-discovery pilot project revealed that many litigants are not diligent about conducting effective meet-and-confer sessions. Even if meetings take place, if inexperienced lawyers did not bring expert assistance, or did not address

45. See section II.A, supra, for further discussion of the Defender Services Office’s National Litigation Support program.

IV. Conclusion

the matters in any depth (a so-called drive-by meet-and-confer), then problems with e-discovery may not have been avoided. Although not every case or lawyer needs these formal meetings, the court can satisfy itself that the parties have worked together to ensure productive access to e-discovery.

At the discovery status conference, the lawyers should provide a discovery disclosure schedule. The judge can clarify what is expected in continued “rolling” discovery, and that disclosure should take place expeditiously, since reviewing e-discovery can be very time-intensive. The court should take this opportunity to advise the parties about their discovery obligations. If the defense will have e-discovery, the court can check if the parties discussed that in the meet-and-confer session; if not, it could order a second meet-and-confer session.

There may be e-discovery issues that the parties have identified but have not been able to solve. If satisfied that they have tried in good faith to settle the matters first, the court can either decide the discovery dispute impromptu, or it can schedule a briefing and a discovery hearing. Subsequent discovery status conferences can be scheduled as needed.

IV. Conclusion

The purpose of this guide is to help judges give guidance and direction to lawyers handling complex criminal electronic discovery. It aims to ensure that the parties manage the case efficiently and thoughtfully, avoid unnecessary delay and costs occasioned by the nature of the e-discovery, and provide defendants full access to the evidence necessary to evaluate the case and make strategic decisions. Of course, this guide cannot answer every e-discovery question that will arise, so judges must be creative in dealing with the myriad of issues that naturally arise in this dynamic field. But this guide does offer an overall framework for addressing criminal e-discovery that can be adapted to virtually every case.

Judges using this publication are encouraged to comment and propose changes to keep it current and relevant.
Appendix A
ESI Protocol Description
Appendix A: ESI Protocol Description

A. ESI Protocol Helps Judges with e-Discovery in Criminal Cases

The ESI Protocol provides practical recommendations to facilitate electronic evidence discovery (e-discovery or ESI) in criminal cases. It seeks to increase efficiency, save money, and reduce litigation over e-discovery issues. To accomplish these goals, the ESI Protocol creates a predictable framework for e-discovery discussions and production, and encourages the parties to resolve e-discovery disputes without court intervention. It was designed to be enduring and flexible by providing both broad principles that will apply regardless of technical changes and detailed guidance that can be updated as technology evolves.

The ESI Protocol has four parts:

1. **Principles:** The 10 Principles are core tenets that set the framework for the recommendations and strategies, and they also serve as a starting place for the uninitiated. A judge can direct a lawyer to begin by reviewing the principles.

2. **Recommendations:** The 10 Recommendations address critical e-discovery topics at a policy level. They are based upon the principles’ core tenets, and they are intended to endure inevitable changes in technology. The recommendations are a framework for informed discussions between the parties about e-discovery issues.

3. **Strategies and Commentary:** The strategies and commentary section addresses the same topics as the 10 Recommendations. It provides practical guidance on key practices. The strategies and commentary will evolve over time in response to changing technology and experience. This section concludes with definitions of e-discovery terms.

4. **Checklist:** This one-page checklist for lawyers and judges identifies the major specific topics to address at a meet-and-confer conference or discovery hearing.
Criminal e-Discovery

B. Overview of the ESI Protocol

Guiding principles. The ESI Protocol is built upon ten principles:

Principle 1: Lawyers have a responsibility to have an adequate understanding of electronic discovery.

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.

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 ongoing dialogue may be helpful.

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.

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
Appendix A: ESI Protocol Description

would do for its own case preparation or discovery production.

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.

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.

Principle 8:

In multidefendant cases, the defendants should authorize one or more counsel to act as the discovery coordinator(s) or seek appointment of a coordinating discovery attorney.

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.
Criminal e-Discovery

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.

Scope. The ESI Protocol is intended only for cases in which the volume and/or nature of the ESI produced as discovery significantly increases the complexity of the case.47 For example, cases involving a large volume of ESI, unique ESI issues, or multiple defendants may benefit from using the ESI Protocol. In simple or routine cases,48 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.49

Limitations. The ESI Protocol does not alter the parties’ discovery obligations or protections under the U.S. Constitution, the Federal Rules of Criminal Procedure, the Jencks Act, other statutes, case law (for example, Brady and Giglio), or local rules.50 It is not intended to serve as a basis for allegations of misconduct or claims for relief, nor does it create any rights or privileges for any party.51 Cases involving classified information have their own unique legal procedures that do not fit within the ESI Protocol.52 The ESI Protocol applies only to postindictment criminal discovery, not civil litigation or preindictment investigations, both of which are governed by existing legal standards.53

An integrated process, not rules to be enforced. The ESI Protocol envisions a collaborative approach to e-discovery based upon

---

47. ESI that is contraband (e.g., child pornography) requires special discovery procedures. See ESI Protocol, Recommendations at 2.
48. Even small amounts of ESI in an unusual or difficult format can increase the complexity of e-discovery, which would counsel using the ESI Protocol.
49. See ESI Protocol, Recommendations ¶ 2.
50. ESI Protocol, Recommendations ¶ 3.
51. Id.
52. ESI Protocol, Recommendations ¶ 5.
the mutual and interdependent responsibilities of the opposing parties. As such, the ESI Protocol sets forth best practices for litigants, not a set of enforceable rules.

**Balancing competing goals.** As with the criminal discovery rules, the ESI Protocol seeks to balance competing goals. For example, to promote cost savings, the ESI Protocol states that if the producing party elects to process ESI for its own case preparation or discovery production, then the results of that processing should—unless they constitute work product—be produced in discovery to save the receiving party the expense of replicating that work. An illustration would be that if the producing party scans paper documents to a TIFF image and OCR text, then those should be provided in discovery rather than providing only the paper documents. Nonetheless, the producing party’s work product—for example, issue tags or document notes—should not be produced. Importantly, the producing party should not be required to take on substantial additional processing or format-conversion costs and burdens beyond what it has already done or would do for its own case preparation or discovery production.

**No easy solutions.** A natural human tendency when confronted with complex problems is to look for easy solutions. But the ESI Protocol recognizes that at this point in the evolution of e-discovery, there is no easy, one-size-fits-all solution.

**Coordinating discovery for multiple defendants.** In multiple-defendant cases, the ESI Protocol recommends that the defendants authorize one or more defense counsel to act as the discovery coordinator or seek the appointment of a coordinating discovery attorney (CDA). CDAs are Defender Services Program—contracted attorneys who have technological knowledge and experience, resources, and staff to assist with the effective management of complex e-discovery.

**Communication, not litigation.** To reduce costs and save time, the ESI Protocol avoids a purely adversarial and rules-driven approach to e-discovery. First, the ESI Protocol recommends that the parties meet and confer at the outset of a case. Second, it recommends

---

55. For more information on coordinating discovery attorneys, see section III.A, supra, at pp. 14–15.
Criminal e-Discovery

communication as a precondition to filing a motion about an e-discovery issue. An aggrieved party is directed to confer with opposing counsel in a good-faith effort to resolve the dispute, and to involve individuals with sufficient knowledge to understand the technical issues, or sufficient authority to settle the dispute cooperatively, before filing any motions. If a motion is filed, the ESI Protocol suggests including a statement of counsel for the moving party stating that, after consultation with the opposing party, they have been unable to resolve the dispute without court action.

Each U.S. Attorney’s Office and Main Justice criminal component has one or more criminal discovery coordinators who are responsible for providing guidance to prosecutors on criminal discovery topics. Each federal and community defender office has IT or other staff and access to the National Litigation Support Team that can provide technical assistance in resolving discovery issues. Lawyers can take advantage of these resources to understand technical issues and facilitate meaningful discussion that may avoid or resolve conflicts.

To avoid unnecessary motions practice, the ESI Protocol calls for supervisor participation in resolving disputes and recommends that prosecutors and federal and community defender offices institute internal procedures that require line prosecutors and defenders to: (1) seek a supervisor’s assistance in resolving an e-discovery dispute, (2) consult with supervisors before filing motions seeking judicial resolution of an e-discovery dispute; and (3) obtain a supervisor’s authorization before alleging that opposing counsel has engaged in any misconduct, abuse, or neglect concerning the production of ESI. These recommendations were included to ensure that the parties explored technological and pragmatic solutions before resorting to e-discovery litigation. Of course, the recommendations for consulting with, or obtaining approval of, a supervisor do not apply to CJA or privately retained counsel.

Whether the ESI Protocol’s meet-and-confer approach will succeed in our adversarial system will depend in some measure upon whether judges encourage the parties to follow the ESI Protocol. At the least, the involvement of technically knowledgeable personnel should help to avoid disputes based on technological misunderstandings.
Appendix A: ESI Protocol Description

**Parties are responsible for identifying and solving e-discovery issues.** The ESI Protocol identifies the responsibilities of both parties. Some examples follow.

**Both Parties**

- When gathering ESI, think about the nature, volume, and mechanics of managing ESI.\(^{56}\)
- Conduct a meet-and-confer to discuss e-discovery issues, and address eighteen specified topics as necessary.\(^{57}\) Use the one-page checklist to help identify possible issues.
- Discuss any issues concerning information provided in discovery that implicates any privilege or that is protected as confidential or personal identifying information.\(^{58}\)
- Discuss a reasonable schedule for producing e-discovery.\(^{59}\)
- Discuss e-discovery security if either party intends to make discovery electronically available to others.\(^{60}\)
- Discuss protective orders if needed.\(^{61}\)
- Memorize any e-discovery agreements.\(^{62}\)
- Give the court advance notice of any issues that will significantly affect the production or review of e-discovery, the need to request supplemental funds, or the scheduling of pretrial motions or trial.\(^{63}\)

---

56. ESI Protocol, Strategies ¶ 2.
57. ESI Protocol, Strategies ¶ 5.
58. ESI Protocol, Strategies ¶ 5(e).
60. ESI Protocol, Strategies ¶ 5(p).
61. ESI Protocol, Strategies ¶ 5(q).
63. ESI Protocol, Strategies ¶ 5(s).
Criminal e-Discovery

Producing Party

- When possible, produce ESI as processed to save the receiving party the expense of replicating the processing.\(^{64}\)
- Create a table of contents.\(^{65}\)
- Give the receiving party an estimate of discovery volume.\(^{66}\)
- Identify any third-party ESI according to which device it came from.\(^{67}\)
- Produce third-party ESI in the format it was received or in a reasonably usable format.\(^{68}\)
- Produce discoverable materials generated by a party during its investigation in a searchable and reasonably usable format.\(^{69}\)
- Produce a cover letter to accompany e-discovery that describes the number of media, the unique identifiers of the media, a brief description of the contents including a table of contents if created, and any Bates ranges or other unique production identifiers.\(^{70}\)

Receiving Party

- Inspect e-discovery promptly after its receipt and give notice to the producing party of any production issues or problems that may impede using the e-discovery.\(^{71}\)

---

\(^{64}\) ESI Protocol, Recommendations ¶ 6.
\(^{65}\) ESI Protocol, Strategies ¶ 5(b).
\(^{66}\) ESI Protocol, Strategies ¶ 5(h).
\(^{67}\) ESI Protocol, Strategies ¶ 5(l).
\(^{68}\) ESI Protocol, Strategies ¶ 6(g).
\(^{69}\) ESI Protocol, Strategies ¶ 6(h).
\(^{70}\) ESI Protocol, Strategies ¶ 7(c).
\(^{71}\) ESI Protocol, Strategies ¶ 5(o).
Appendix B
ESI Protocol
Appendix B: ESI Protocol

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 Electronic Technology Working Group (JETWG)

February 2012
Appendix B: ESI Protocol

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 the U.S. Courts, Defender Services Office (DSO), the Department of Justice (DOJ), Federal Public and Community Defender Organizations (FPDOs and CDOs), 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.
Criminal e-Discovery

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 ongoing 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.)
Appendix B: ESI Protocol

**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 multidefendant cases, the defendants should authorize one or more counsel to act as the discovery coordinator(s) or seek the 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 and secure, and less costly.
Criminal e-Discovery

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 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;

72. 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.
Appendix B: ESI Protocol

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; 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 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. 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.

73. 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.

74. 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, nonstandard and proprietary software formats; and/or (3) multiple-defendant cases accompanied by a significant volume of ESI.
Criminal e-Discovery

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 ongoing 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.
Appendix B: ESI Protocol

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 as follows:

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.75

b. ESI received from third parties should be produced in the format(s) it was received or in 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 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 be-

---

75. An example of a format of production might be the production of 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.
cause 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 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 reduced 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.
Appendix B: ESI Protocol

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,76 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.

c. To avoid unnecessary litigation, prosecutors and Federal Defender Offices77 should institute procedures that re-

76. Coordinating Discovery Attorneys (CDAs) 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. Attorney’s 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.

77. For private attorneys appointed under the Criminal Justice Act, this subsection (c) is not applicable.
**Criminal e-Discovery**

quire 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, pri-
Appendix B: ESI Protocol

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 contain additional guidance in sections 5(f), 5(p), and 7(e).
Criminal e-Discovery

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 e-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 wiretap information* (audio recordings, transcripts, line sheets, call reports, court documents, etc.)

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

ix. *Tests and examinations*

x. *Experts* (reports and related information)

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

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

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

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

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 dis-
Criminal e-Discovery

discovery. In complex discovery cases, a table of contents to the available discovery materials can help expedite the opposing party’s review of discovery, promote early settlement, and avoid discovery disputes, unnecessary expense, and undue delay. Because no single table of contents is appropriate for every case, the producing party may devise a table of contents that is suited to the materials it provides in discovery, its resources, and other considerations.

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

d. **Proprietary or legacy data.** Special consideration should be given to data stored in proprietary or legacy sys-

---

78. 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).

79. 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.

80. 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.
Appendix B: ESI Protocol

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

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

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

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

h. **ESI discovery volume.** To assist in estimating the receiving party’s discovery costs and to the extent that the producing party knows the volume of discovery materials

---

81. Attorney–client and work-product issues (see, e.g., F. R. Crim. P. 16(a)(2) and (b)(2)) 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.

82. 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.

83. Because pretrial detainees often are held in local jails (for space, protective custody, cost, or other reasons), which 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.
Criminal e-Discovery

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

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

j. **Paper materials.** 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
Appendix B: ESI Protocol

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

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

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

---

84. 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.
**Criminal e-Discovery**

being discussed, what the producing party has agreed to produce, and any known problems or gaps in the metadata received from third parties.

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

**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;\(^{85}\)

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

---

85. The parties should consult their litigation support personnel concerning encryption or other security options.
Appendix B: ESI Protocol

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

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

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

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, 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 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.

---

86. 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.

87. 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.
Criminal e-Discovery

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,\(^88\) 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,\(^89\) made available for inspection, or, if they have already been converted to digital format, 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 elec-
Appendix B: ESI Protocol

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.\textsuperscript{90}

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

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 into 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 (\textit{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, \textit{e.g.}, parent–child relationships.

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

\textsuperscript{90} 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.
Appendix B: ESI Protocol

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
Criminal e-Discovery

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 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 reasonably usable form(s). The parties should explore what formats of production 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.

t. **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),

---

91. An example of a format of production might be the production of 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.
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 more cost-effectively utilized.92

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.

---

92. For guidance on making computer-generated versions of investigative reports and witness interview reports, see the description of production of TIFF, PDF, and extracted text formats in paragraphs (b)(ii)(1) and (ii).
Criminal e-Discovery

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.\(^{93}\) 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 identifiers, 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.

---

\(^{93}\) 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.
Appendix B: ESI Protocol

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

i. *Not appropriate for email transmission:* Certain categories of ESI discovery are never appropriate for email transmission, including, but not limited to, certain grand jury materials; materials affecting witness safety; materials containing classified, national security, homeland security, tax return, or trade secret information; or 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.\(^\text{94}\)

8. **Coordinating Discovery Attorney**

Coordinating Discovery Attorneys (CDAs) are AOUSC-contracted attorneys who have technological knowledge and experience, resources, and staff to effectively manage complex ESI in multiple-defendant cases.

---

\(^{94}\) 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).
**Criminal e-Discovery**

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 U.S. Attorney’s 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.

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 online banking.

b. **Coordinating Discovery Attorney (CDA).** An AOUSC-contracted attorney who has technological know-
Appendix B: ESI Protocol

ledge 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 en-
Criminal e-Discovery

tire 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 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 TIFFs and PDFs. Document images, such as TIFFs and PDFs, 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, paths 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
Appendix B: ESI Protocol

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 50–98% 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.
Criminal e-Discovery

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 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?
Appendix B: ESI Protocol

☐ 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 third-party digital devices?
☐ Forensic images of ESI digital devices?
☐ Metadata in third-party ESP?
☐ 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, 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?
Appendix C
First Appearance e-Discovery Colloquy
Appendix C: First Appearance e-Discovery Colloquy

At the first appearance of a defendant and after appointment of counsel, engage parties in the following colloquy concerning e-discovery.

A. Ask the prosecutor about possible e-discovery in the case, and generally how the government will proceed:
   1. Does the government intend to produce any discovery in electronic formats?
   2. Does the volume or nature of the government’s electronic discovery significantly increase the complexity of the case?
   3. Are you familiar with the ESI Protocol?
   4. Are you going to utilize the ESI Protocol?

B. Ask defense counsel about familiarity with managing e-discovery, and generally how the defense will proceed:
   1. Are you familiar with the ESI Protocol?
   2. Do you have a copy of the ESI Protocol to rely on as you work through the e-discovery? If not, the government can provide a copy.
   3. What is your experience with complex e-discovery cases?
   4. Are you familiar with various software products and e-discovery services that can be used to review and organize e-discovery? Have you used them before?
   5. Have you worked with litigation support, paralegals, or IT staff before to review e-discovery?
   6. Do you presently have litigation support, paralegals, or IT staff who can work with you to review and organize electronic evidence? If not, you may need to decide what type of expert or experts you will need. Do you know how to do that?
Criminal e-Discovery

C. Engage both parties in a discussion of how they will cooperatively address complex e-discovery:

1. Are you utilizing the ESI Protocol?
2. Have you already had a meet-and-confer to address e-discovery issues? If so, do you have any agreements or a discovery plan? If not, what is your plan for addressing e-discovery issues?
3. Will the volume or nature of the e-discovery potentially affect:
   a. Speedy trial deadlines for this case?
   b. Scheduling pretrial motions?
   c. Scheduling trial?

D. Address all attorneys about what the court expects of them in managing a complex e-discovery criminal case:

1. I expect you already have, or will promptly gain, an adequate understanding of and adequate technical assistance in e-discovery matters.
2. I expect the lawyers on this case to manage electronic discovery effectively, efficiently, and responsibly, and to seek cost savings.
3. I also expect the lawyers on this case to determine what software programs and expert assistance you need to review the discovery. If you do not know what type of expert to retain or what software programs to use, you should consult with someone knowledgeable about e-discovery before making those decisions.
4. While the lawyers may, and should, employ litigation support, paralegals, and/or IT staff, ultimately, the lawyers are responsible for e-discovery decisions made in this case.
5. I encourage all parties to utilize a collaborative approach to e-discovery based upon the mutual
Appendix C: First Appearance e-Discovery Colloquy

and interdependent responsibilities of the opposing parties. The ESI Protocol offers a model of such an approach.

6. An important part of the process is a meet-and-confer discussion about the e-discovery issues in this case. I encourage you to use the checklist at the end of the ESI Protocol during your meet-and-confer session. For scheduling purposes, some of the key steps to pay attention to are:

   a. The parties should discuss a reasonable e-discovery production schedule.

   b. Defense counsel should be proactive about testing the accessibility of the e-discovery production when it is received, and promptly notify the government of any problems in accessing the materials.

   c. If defense counsel determines that additional funds for expert assistance are needed, that needs to be brought to the court’s attention promptly.

7. I expect that the parties will promptly notify the court of any e-discovery issues that might reasonably affect speedy trial deadlines, or the scheduling of pretrial motions or trial.

E. If there are CJA attorneys appointed to defend one or more defendants, address funding issues with them:

   1. If you will be hiring expert assistance to organize and review the e-discovery, have them help you decide on a realistic estimation of the time that they will need to do so. If that exceeds the expert’s costs “cap,” file an ex parte, sealed motion asking to exceed the capped amount, explaining the work that would be done and how you or they arrived at that cost estimate.
Criminal e-Discovery

F. If there are multiple defendants (so multiple defense counsel) in the case, the advisability of coordinating e-discovery among defendants should be raised at the first appearance. This gives counsel time to discuss and decide potential coordination before a meet-and-confer session.

1. I am not ordering you to do this, but you may want to consider whether to designate one defense attorney to manage e-discovery.

G. Advise defense counsel about the availability of resources to help guide them in managing complex e-discovery:

1. If you need advice and guidance about getting started, there are resources available to help you decide how to productively get the information you need from the e-discovery. The National Litigation Support Team, part of the Defender Services Office (DSO) of the Administrative Office of the U.S. Courts,⁹⁵ is available to provide guidance about how to efficiently, and cost-effectively, manage e-discovery. If you are not familiar with the technology and expert assistance you will need, you should contact them right away, well before the meet-and-confer session. They can also tell you about contracts they have secured for reduced prices on some of the software programs that may help you review and organize the evidence.

2. Another resource available to defender offices and CJA counsel is appointment of a coordinating discovery attorney. Those handling voluminous or complex e-discovery (especially when there are multiple defendants) can have an attorney expert in e-discovery appointed to work with defense counsel to help coordinate, organize, and process e-discovery. After exploring the nature and vol-

⁹⁵ The National Litigation Support Team can be contacted at (510) 637-3500.
Appendix C: First Appearance e-Discovery Colloquy

ume of e-discovery, and what it will take for defense counsel to review it, if you think this case needs a coordinating discovery attorney appointed, then file an ex parte sealed motion explaining why, and the court will consider it.

H. Finally, the court may decide to set a discovery status conference (giving parties enough time to secure expert assistance if needed, and to hold a meaningful meet-and-confer session) to verify that e-discovery is moving smoothly, cooperatively, and effectively. Inform all parties:

1. I am going to schedule a discovery status conference to follow up on the progress the parties are making with the e-discovery, and ensure that any problems with it are resolved early.

2. I encourage you to conduct your meet-and-confer session well before the discovery status conference so that you can address and resolve any issues.
Appendix D
Discovery Status Conference e-Discovery Colloquy
Appendix D: Discovery Status Conference e-Discovery Colloquy

Having already addressed e-discovery issues at the first appearance, the court may schedule a discovery status conference to confirm whether e-discovery is being addressed by parties intelligently, efficiently, and cost-effectively. At a discovery status conference, engage parties in the following colloquy concerning the status of their e-discovery.

A. In cases with multiple defendants, the court would have asked parties to consider whether one defense attorney should be responsible for receiving, distributing, and possibly coordinating work on e-discovery for all defense teams. The court can follow up on that by asking all multiple-defense counsel:

1. Is this a case where management of the e-discovery would benefit from having either:
   a. A single defense attorney receiving e-discovery from the government for all defendants and being responsible for disseminating it to all defendants; or
   b. A coordinating discovery attorney appointed by the court?

2. If one of you will manage the discovery for all defendants, have you already selected that attorney? If you want to use a coordinating discovery attorney, have you contacted the National Litigation Support Team to ensure that doing so is appropriate for this case?

B. The court can then check on the parties’ success in trying to decide and resolve e-discovery issues. To that end, it should address both parties:

1. Did the parties conduct a meet-and-confer session?
2. Did you utilize the ESI Protocol?
3. Did you have litigation support specialists (if needed) to help you decide how to manage the ESI di-
Criminal e-Discovery

discovery? Did you have your litigation support specialists with you at the meet-and-confer session?

4. Were the parties able to reach decisions as to when, how, and in what format the e-discovery will be produced?

5. Were the parties able to reach decisions on other e-discovery issues (such as those listed in the checklist of the ESI Protocol)?

C. Verify with the government whether there is an e-discovery production schedule agreed upon:

1. Do you have an e-discovery production schedule?
   a. What is it?
   b. Have you started producing e-discovery to the defense?
   c. Do you anticipate a “rolling” production of e-discovery?

D. The court can also verify with the defense whether it has performed an initial review of any disclosures to ascertain that it can access and utilize the ESI. Then the court should inquire of defense counsel whether the defense has an e-discovery production schedule that was agreed upon:

1. Do you have a schedule as to when you will do a summary initial review of the e-discovery (to ascertain that you can open and use it as produced)?
   a. What is it?
   b. If production has started, have you performed a review of the e-discovery to verify that you can access and use it?

2. You may have e-discovery to disclose to the government. Did you already discuss any defense e-discovery in the meet-and-confer session?

3. Do you have an e-discovery production schedule?
Appendix D: Discovery Status Conference e-Discovery Colloquy

a. What is it?
b. Have you started producing e-discovery to the government?
c. Do you anticipate a “rolling” production of discovery?

E. If the parties did not accomplish all that was necessary, the court may want to reiterate to all parties some of its advisements about expectations and resources from the First Appearance e-Discovery Colloquy, sections D–G, contained in Appendix C.

F. The court may decide to inquire about any unresolved discovery issues or disputes. If so, it could ask both parties:

1. Were all e-discovery issues resolved by the meet-and-confer session? Were there any e-discovery issues that were not resolved?

G. If there are unresolved issues, the court may want to set another discovery status conference to settle those matters.
The Federal Judicial Center

Board
The Chief Justice of the United States, Chair
Judge Catherine C. Blake, U.S. District Court for the District of Maryland
Judge Curtis L. Collier, U.S. District Court for the Eastern District of Tennessee
Magistrate Judge Jonathan W. Feldman, U.S. District Court for the Western District of New York
Judge Kent A. Jordan, U.S. Court of Appeals for the Third Circuit
Judge Michael J. Melloy, U.S. Court of Appeals for the Eighth Circuit
Judge Kimberly J. Mueller, U.S. District Court for the Eastern District of California
Chief Judge C. Ray Mullins, U.S. Bankruptcy Court for the Northern District of Georgia
James C. Duff, Director of the Administrative Office of the U.S. Courts

Director
Judge Jeremy D. Fogel

Deputy Director
John S. Cooke

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center’s Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training for judges and court staff, including in-person programs, video programs, publications, curriculum packages for in-district training, and Web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center’s research also contributes substantially to its educational programs. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and informs federal judicial personnel of developments in international law and other court systems that may affect their work. Two units of the Director’s Office—the Information Technology Office and the Editorial & Information Services Office—support Center missions through technology, editorial and design assistance, and organization and dissemination of Center resources.
1. **Discovery Received from Government**
   a. All discovery and any case related documents should be stored on a network drive that is accessible to everyone on the legal team. Any original documents, hard drives or CD's should be given to the designated legal assistant or paralegal to store for the duration of the case.
   b. All documents should be searchable.
   c. A folder structure and file naming protocol should be set and agreed upon by team members
      i. The network folder structure should be similar to “CASES\Jones, Tucker\Discovery\2017_02_21 Production”
      ii. File naming protocol
         1. If the discovery is received in electronic format
            a. The file name should be kept in the original format
               i. If the government file name is D-000001 – D-000100, it should be saved as “CASES\Jones, Tucker\Discovery\2017_02_21 Production/D-000001-D-000100”
         2. If the discovery is received in paper format
            a. The file name should be similar to the electronic file naming convention or (if applicable) by Bates Number (D-000101)
      iii. A separate folder should be kept for Discovery letters
         1. The discovery folder structure would be similar to the network folder structure “CASES\Jones, Tucker\Discovery\Discovery Letters”
      iv. It may be useful to keep an electronic Discovery log to track when discovery is received and what (if applicable) Bates range is received

<table>
<thead>
<tr>
<th>DATE RECEIVED</th>
<th>BATES RANGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/15/2017</td>
<td>D-000001-D-000100</td>
<td>PDF Discovery and Some Media Files</td>
</tr>
<tr>
<td>2/18/2017</td>
<td>D-000101-D-000105</td>
<td>Audio Recordings</td>
</tr>
<tr>
<td>2/21/2017</td>
<td>D-000106-D-000137</td>
<td>Transcripts</td>
</tr>
</tbody>
</table>

d. **Discovery received Pre-Trial**
   i. When discovery is received, the attorney will give the discovery to the Legal Assistant or Paralegal to handle
ii. Electronic (CD, DVD, Hard Drives or other electronic storage device)
   1. Legal Assistant or Paralegal should check the PDF discovery to make sure it is searchable
      a. If discovery is not searchable, it should be OCR’d
   2. Record the information in the Discovery Log

iii. Paper
   1. Should be scanned into PDF files maintaining (if possible) document breaks
   2. Save PDF files to the Case file using the proper naming protocols
   3. PDF files should be OCR’d and made searchable
   4. All documents from the government should contain a Bates Number
      a. If the documents do not contain a Bates Number
         i. Ask the government to reproduce with a Bates Number
         ii. If they will not reproduce, add a Bates Number and notify the government that Bates Numbers were added and the system used. Give the government a copy of the documents with the Bates Numbers.
   5. Record the information in the Discovery Log

ii. Discovery received during Trial
   i. Paper
      1. If necessary, copies should be made as soon as possible for the attorney(s) to use as working copies during the trial.
      2. Scan into PDF and save to the designated network folder
         a. OCR
      3. Record the information in the Discovery Log
   ii. Electronic
      1. If necessary, print out copies as soon as possible for attorney(s) to use as working copies during the trial.
      2. Save a copy to the designated network folder
      3. Record the information in the Discovery Log

2. Suggested use of Software for Discovery Management
   a. dtSearch
      i. A search and retrieval software program. It allows users to quickly search electronic computer files. Before you are able to search your documents, dtSearch must index them and the PDF documents must be searchable. Indexing is the process of reading through each document and creating special files which hold information about the words within all of those documents. When you perform a search, dtSearch queries the index, not
the documents themselves. This is why it can return results so quickly. Documents do not need to be formatted in any special way. The original documents do not need to be moved or copied for dtSearch to index them.

b. Adobe Acrobat Pro
   i. Acrobat allows us to view, create, search and manage files in the Portable Document Format (PDF)
   ii. Acrobat will also make non searchable PDF’s searchable

3. All other case related Documents
   a. Documents should be stored in the designated network drive
   b. Folder structures should be agreed upon for documents
      i. Investigation Records “CASES\Jones, Tucker\Investigation Records”
      ii. Client Correspondence “CASES\Jones, Tucker\Client Correspondence”

4. Trial Preparation
   a. Determine if Trial Director will be utilized
   b. Defense Exhibits
      i. Check if the Judge has any specific rules about
      ii. Identify potential documents at least one week in advance
      iii. Determine how many “Paper” sets of Exhibits will be needed
         1. Check if the government will accept an electronic copy of Defense exhibits, this will avoid having to make an additional “Paper” set for them
      iv. Identify what numbers will be used for Exhibits and how documents should be marked
      v. Prepare Exhibit List
         1. Microsoft Word
         2. Microsoft Excel
            a. Using an Excel spreadsheet can be useful when having to quickly make changes to Exhibit numbers and items
   vi. Prepare Exhibit Tags

<table>
<thead>
<tr>
<th>Ex. #</th>
<th>Description</th>
<th>Bates No.</th>
<th>Identified</th>
<th>Admitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>Surveillance Video without Audio</td>
<td>D-0000054</td>
<td></td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>Surveillance Video with Audio</td>
<td>D-0000063</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>Jail Call 9/16/03</td>
<td>D-0000062</td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>Jones Injury Report</td>
<td>D-0000028</td>
<td></td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Brownson Injury Report</td>
<td>D-000015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Jones X-Ray</td>
<td>D-000044</td>
<td></td>
<td></td>
</tr>
<tr>
<td>107</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
c. Government Exhibits
   i. Ask for the government’s exhibits in advance
      1. Request an electronic copy of the exhibits for use in Trial Director
d. Trial Director
   i. Determine who will running the Trial Director software during Trial
   ii. Review what exhibits will need to be displayed in court
      1. If there are a large number of Exhibits, it will ensure that only the
         necessary exhibits be loaded into Trial Director
      2. Will ensure that the proper exhibit numbers are communicated
         and displayed in court
      3. If audio or video files are used
         a. Make sure that the files are cut to display on the portion
            necessary
   iii. Rename the documents so the file name is the Exhibit Number
      1. Example “101”
         a. Using simple file names will make calling up an Exhibit in
            Trial Director easier and more streamlined
   iv. If possible, do a practice run through of Trial Director
      1. This allows the attorney to see how exhibits are displayed and if
         they want something called out or zoomed in
      2. Allows the person running Trial Director to practice calling up
         exhibits and zooming in and making call outs where needed
e. Determine if PowerPoint will used for Opening and/or Closing
   i. Determine what exhibits, documents or files will be used
      1. Often Audio and Video files need to be reformatted or changed to
         display and play properly in PowerPoint
      2. If possible, do a practice run of the presentation
         a. This ensures slides are in the correct order
         b. Ensures the correct exhibits are in the presentation
f. Schedule a time with the Court to set up equipment
   i. Make sure computer and all equipment is in working order
   ii. Ensures proper display of Trial Director and PowerPoint on the
       courtroom display screens
Cloud Computing, Storing, and Sharing: 
Guidance for the Solo and Small Firm Lawyer 
By Donna Lee Elam and Sean Broderick

Most of us went to law school to become trial lawyers, not “techies.” But with the explosion of technology offering such attractive services, lawyers who had once approached IT with “fear and loathing” are overnight embracing it. From reading and sending e-mails using Gmail, to conducting legal research using Westlaw or LexisNexis, to preparing briefs using Microsoft Office 365, solo practitioners and large firms alike have quickly adopted cloud technology. The cloud offers many benefits, but it also presents a number of potential pitfalls to unwary, inexperienced practitioners.

Benefits and Pitfalls of Cloud Storage
Confronting increasing volumes of information in their cases, lawyers have realized that the cloud can improve their efficiency, allow for greater flexibility, and reduce costs. Cloud storage is especially attractive. For small firm practitioners with little to no IT support, free to low-cost cloud storage services like Dropbox and Box.com are far cheaper than adding computers to the office, and require no tech capabilities. Providers tend to charge for the services used, and customers can turn apps on and off as needed. (See ARMA INT’L, GUIDELINE FOR OUTSOURCING RECORDS STORAGE TO THE CLOUD (2010).) Lawyers can expand their cloud storage with the click of a button and not have to worry about buying new hardware or learning how to create a network.

Cloud storage also allows attorneys greater options in accessing files. They can reach their data anytime from anywhere in the world, regardless of whether they are on an office computer, laptop, tablet, or smartphone. Moreover, other people can be given secure access to cloud-stored information (e.g., clients, experts, investigators, and co-counsel) without having to let them breach the firm’s firewall.

Particularly popular is how cloud files are immediately updated or synced so that anyone accessing them from any device automatically reaches the most recent version of a document. Because attorneys often collaborate with others in different offices, the ability to share and sync files with them makes cloud storage a premium. In fact, many services (for example, Microsoft Office 365) let multiple individuals work on the same document concurrently, allowing for same-time group editing.

Cloud computing companies also offer the most recent versions of a variety of software programs to their users. In fact, many providers simply offer “software as a service,” allowing their customers to pay by subscription or hourly for using particular programs. That way, lawyers can open virtually any file without having to purchase and install the software on their office system. NetDocuments, for instance, can be used with every major file type and employ that file’s originating program; in other words, lawyers can continue drafting in the cloud in the program in which that document was created, so that it does not have to be “translated” to another program (such as from WordPerfect to Word) in order to revise it in the cloud. This service also allows lawyers to “test drive” a program to see if they like it before purchasing it.
Despite the tremendous utility of cloud storage, control and protection of data in the cloud is necessarily entrusted to an outsider. The cloud provider’s security and reliability will always be serious matters to consider due to security concerns and a number of data breaches within cloud storage services. Dropbox, the most popular of the current cloud storage services, has had several reported security glitches. In 2011, when it had more than 25 million users, Dropbox reported that a “code update” programmer error caused a temporary security breach that allowed any password to be used to access any user account for four hours. In 2012, a stolen password was used to access an employee’s Dropbox account that contained a document listing a number of Dropbox users’ e-mail addresses. Most recently, in May 2014, a flaw was discovered that allowed unauthorized users to gain access to Dropbox and Box.com, another popular cloud storage service. Outsiders could access users’ confidential files such as tax returns, bank records, and mortgage applications. (Dave Lee, *Warning over Unintentional File Leak from Storage Sites*, BBC NEWS (May 6, 2014), suggests that outsiders’ ability to access the files was “an unexpected consequence of user behaviour,” i.e., the creation of public links to the files.)

Cloud services may also suffer from reliability issues. The companies could fail given the competitive market and emergence of new technologies. For example, in September 2013, cloud storage provider Nirvanix went out of business, giving customers only two weeks to remove their data. In the event of bankruptcy, shutdown, or corporate takeover, users may lose or temporarily lose touch with their data. For instance MegaCloud, a provider of free and paid consumer cloud storage, shut down without warning in late October 2013, with users complaining of not being able to access their data on social media sites in the days that followed. For that reason, lawyers may want to check the cloud company’s credit worthiness before signing on with it. Furthermore, because global cloud services maintain servers abroad, their data may be wiped out by foreign acts of war and terrorism. Moreover, cloud services that depend on the Internet will inevitably be “down” periodically when the provider’s Internet connections fail.

Many cloud services are global with servers located throughout the world. They are consequently subject to foreign laws, so privacy and accessibility laws could be quite different from what Americans have come to rely on.

**Ethics Obligations in Using Cloud Technology**

A major concern of resorting to cloud computing and storing is ethical duties that every lawyer must observe. Ethics obligations to maintain competency and protect client confidentiality may be impacted when using the cloud. Consequently, it is important that cloud consumers use it intelligently and take reasonable measures to safeguard client data in it.

In 2012, the ABA changed its model ethics rule regarding competence by commenting that the obligation to maintain competency also extends to “keep[ing] abreast of changes in the law and its practice, including the *benefits and risks associated with relevant technology.*” (MODEL RULES OF PROF’L CONDUCT R. 1.1 cmt. [8] (emphasis added).) State bars started to follow suit. (See, e.g., ARIZ. RULES OF PROF’L CONDUCT R. 1.1 cmt. 6 (Jan. 1, 2015, adopting ABA Model Rule comment); PA. RULES OF PROF’L CONDUCT R. 1.1, 1.6(d) (amended Nov. 21, 2013).) This means that lawyers must have a basic working knowledge of how to take advantage of technological developments—including using the cloud—in representing their clients.

Additionally, as part of their duties to competently use modern technology, lawyers who engage third parties to provide outsourced services are responsible to some degree for the third parties’ conduct. Model Rule 5.3 provides, “[A] lawyer shall be responsible for conduct of [a nonlawyer retained by that lawyer] that would be a violation of the Rules of Professional
Conduct if engaged in by a lawyer.” Because cloud storage is a form of outsourcing, attorneys must be mindful that they remain ultimately responsible for the conduct and use of cloud storage providers. (See Pa. Bar Ass’n Comm. on Legal Ethics & Prof’l Responsibility, Formal Op. 2011-200 (Nov. 2011) (“Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property”).) Therefore, they should make reasonable efforts to ensure that their cloud service is compatible with their obligations to provide direct supervisory authority over cloud providers. (See ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (Aug. 5, 2008) (“Lawyers’ Obligations When Outsourcing Legal and Nonlegal Support Services”).)

The other ethical quandary lawyers face in the cloud is ensuring that client confidentiality is not violated. (Toby Brown, Use Gmail—Waive Privilege?, 3 GEEKS & A L. BLOG (Aug. 19, 2009), http://tinyurl.com/kkuguv.) Attorneys can retain service providers—like retaining experts—and the work they provide falls under the confidentiality umbrella of the firm. Hence, placing client communications and work product in the hands of a third-party cloud company is not necessarily a violation of Model Rule 1.6. (Donna Lee Elm & Sean Broderick, Third-Party Case Services and Confidentiality, CRIM. JUST., Spring 2014, at 15.) Nonetheless, that depends on choosing a cloud provider that has adequate security protections in place, or drafting a service level agreement (SLA) that spells out access, ownership, and notice about security breaches. Absent due diligence in setting up adequate safeguards, a lawyer is at risk of negligently exposing clients’ confidences.

Ethics considerations regarding cloud computing and storage services do not mean they cannot be used. The benefits are too great to ignore, and the change in Model Rule 1.1 indicates that lawyers are now expected to have some minimal understanding of cloud offerings whether they use them or not. Small firm practitioners who decide to use cloud services, but want to avoid running afoul of their ethics obligations or encountering security and reliability pitfalls, need some practical guidance.

**Best Practices for Cloud Provider Selection**

Small firms often do not have the IT staff or resources to invest in creating their optimal cloud solution. But there are some basic steps they can take, requiring minimal technology experience, to meet the competency and confidentiality duties and avoid common pitfalls in selecting and utilizing cloud programs.

**Understand the SLA and company policies.** This calls for a due diligence review. Thoughtfully read the SLA to ensure that client data can be adequately protected and maintained in the cloud. Watch for:

- Who owns the data? Because the provider often owns it, look for a company whose agreement clearly states that the attorney/firm owns the data. (See Gil Press, Do You Know Where Your Data Is and Who Reads It? Varonis Knows, FORBES, Oct. 21, 2013, http://tinyurl.com/ortmwak.)
- Who can access the data? The agreement should ensure that access is kept to a minimum, and specify which employees will have access as well as which ones are prohibited from viewing file contents.
- Do they adequately preserve the data’s confidentiality and security? Besides hacking security, do they encrypt the data when it is in storage or being transmitted?
How do they guarantee the availability of your files? They should have a robust file backup and recovery plan.

What notice will they provide if the data is subpoenaed? Confirm their obligation to notify customers immediately of any legal attempts to access data, specifying what steps will or will not be taken in response, whether the provider will challenge it in court, and allocation of costs involved in litigation and production. Note that the Stored Communications Act, 18 U.S.C. § 2703(b), requires cloud providers to keep government search warrants for customer records secret. (See Steve Kovach, Dropbox: We’ll Turn Your Files Over to the Government If They Ask Us To, BUS. INSIDER (Apr. 18, 2011), http://tinyurl.com/3pksf9e (quoting Dropbox policy: “It is also worth noting that all companies that store user data (Google, Amazon, etc.) are not above the law and must comply with court orders and have similar statements in their respective terms of service.”).)

What happens to data if the service changes hands or goes out of business? Although most companies do not address this issue in their materials or agreements, a prudent consumer will ask a representative this question before signing on.

What are the remedies if the cloud service fails to live up to its promises? Though most companies’ agreements do not address failure contingencies, customers can take extra comfort in those companies that do.

Many cloud services have set SLA terms and will not modify them. But unless you are comfortable with their existing degree of security and restrictions on access to client data, you should not risk violating Model Rule 1.6 by hiring that provider. Also bear in mind that cloud providers’ policies may change over time, so you should periodically check. For instance, in 2012, Dropbox added terms to make it clear that it did not own its customers’ data. (Nilay Patel, Is Google Drive Worse for Privacy Than iCloud, Skydrive, and Dropbox?, THE VERGE (Apr. 25, 2012), http://tinyurl.com/7of7fca.)

Subscribe to a paid version of cloud storage. When using a free cloud service, you may well get what you pay for. Free services may need to shortchange the security and options they offer, or sell your browsing information, in order to stay in business. The apps or programs they provide also often lack the full features and functions of paid versions. Unless you can risk having your cloud data compromised, do not resort to free versions of a cloud storage provider.

Know where the data is stored. Generally, the security and confidentiality of cloud data is governed by privacy and accessibility laws of the jurisdiction where the server holding that data is located. Dropbox files, for example, are maintained in data centers across the United States, whereas Google data centers are located throughout the Americas, Asia, and Europe. (Where Does Dropbox Store Everyone’s Data?, DROPBOX, https://www.dropbox.com/en/help/7 (last visited May 8, 2015); Data Center Locations, GOOGLE DATA CENTERS, http://www.google.com/about/datacenters/inside/locations/ (last visited May 8, 2015).) Foreign data storage locations led to Microsoft’s recent challenge of a government warrant for e-mails residing on its Dublin, Ireland, server. (See Ellen Nakashima, Microsoft Fights U.S. Search Warrant for Customer E-mails Held in Overseas Server, WASH. POST, June 10, 2014, http://tinyurl.com/pnlv8sa.) Some customers also prefer to have their data stored within the United States so that our federal government can intervene if there is a problem with the vendor. But others prefer that their data be stored abroad, perhaps in countries with stricter privacy laws than the United States and that actively resist foreign governments’ subpoenas.
**Review the provider’s uptime.** Cloud services are only as valuable as they are accessible. If a cloud provider relies on an Internet connection that fails from time to time, users will be stranded, unable to reach their data until the system comes back up. Lawyers choosing a provider should inquire into its uptime record, and may want to negotiate more favorable uptime options.

**Ensure that data can be recovered.** Most cloud providers presently use multiple sites to hold the data. Hence if one site goes down, they have the ability to have the server copied or backed up to a different data center, so it can be back in operation in minutes. Cloud providers with that type of configuration are clearly preferable to those without it.

**Confirm adequate cloud security.** Because of obligations to preserve client confidences inviolate, it is critically important to understand what security a particular cloud provider offers. Although service providers fall under the lawyer’s umbrella of confidentiality, if they grant access to any other third party, otherwise privileged information can lose its privilege. Cloud providers should explain their firewalls and what security measures they have taken to detect and stop unwanted intrusion. A good example of what to look for can be seen on the Amazon Web Services website, which provides specific information on a host of security considerations such as secure access, firewalls, and multifactor authentication. *(AWS Security Center, AMAZON WEB SERVICES, http://aws.amazon.com/security/*) Practitioners may instead consider services guaranteeing no access to the data, which are currently on the rise. A prominent example of nonaccess service is SpiderOak, which has zero-knowledge privacy—meaning the server never knows the content of the data being stored. The information is strictly encrypted so the company cannot access it. The downside to this option is that SpiderOak cannot offer any assistance if the customer forgets his or her encryption password. *(See Engineering: The Details Behind What We Do, SPIDEROAK, https://spideroak.com/engineering_matters (last visited May 8, 2015).)*

**Stay abreast of cloud security advances.** Most state bar opinions on cloud computing take into account how technology keeps changing, requiring attorneys to stay informed. In practical terms, this means that lawyers should periodically check the cloud storage service’s security measures. They ought to review settings such as account permissions, backup and restore options, and activity logging/notification—paying special attention to security settings after upgrading to a new version of the operating system. Lawyers should investigate new security options and confirm that security measures that were in place remain intact.

**Ensure security in transit to and from the cloud server.** When data must move across the Internet (as it does in cloud computing), a cautious practitioner will check whether the data is encrypted when traveling to and from the cloud. Confirm that data is encrypted whether it is in motion or at rest. For example, Dropbox uses SSL (keeping transmitted data encrypted) in transit, and uses 256-bit AES encryption when the data is being stored. *(Your Stuff Is Safe with Dropbox, DROPBOX, https://www.dropbox.com/security (last visited May 8, 2015).)*

**Confirm complete data destruction when finished.** Cloud storage providers are far more concerned with *not* losing data entrusted to them than with ensuring that it is completely destroyed when the user is finished. A lawyer should check whether a cloud company has a data return or destruction policy that will ensure client confidentiality.

**Consider client permission to use the cloud.** Some state bars encourage attorneys to obtain their clients’ written, informed consent to use cloud-based services. For instance, the Pennsylvania Bar stated that in some circumstances, “a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider” and a lawyer
“may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client’s matter.” (Pa. Bar Ass’n Comm. on Legal Ethics, Formal Op. 2011-200, at 7 (Nov. 2011).) This step was recommended due to the lack of direct control over the vendor and the unpredictability of technology (including advances, interruptions of service, and loss of data).

**Best Security Practices for Cloud Use**

Some basic practices help small firms ensure security of their confidential data when resorting to cloud computing and storage.

- **Restrict what files will be stored in the cloud.** There may be some files that are so sensitive that even a very small possibility of exposure is unacceptable. They should not be placed in the cloud.

- **At a minimum, encrypt sensitive files.** In addition to security settings, cloud users may be able to encrypt sensitive files. The surest option is to encrypt files on your device before they are sent to the cloud. Otherwise, choose an encryption option offered by the cloud service.

- **Consider using the cloud only for temporary storage.** Although cloud storage can serve as the “backup system” for office computers for some firms, the less confidential information placed in the cloud, the less risk of a catastrophic security breach. If the cloud is used primarily to upload and download documents to and from a client, then creating an automatic deletion policy after a certain amount of time minimizes the risk of hacking those documents.

- **Review security settings on the devices used to access the cloud.** One of the greatest benefits of cloud computing is the ability to access the stored data from a large number and variety of devices. Security of cloud data, then, also depends on security of the devices transmitting and accessing the cloud data. The security options often differ between work computers, home computers, tablets, mobile devices, and the specific web browsers used on each device. A user’s security options may also vary depending upon how he or she accesses cloud storage.

  What options to use may be specific to the device, operating system, and web browser. For examples of options available on a Windows machine, see *Understanding Security and Safe Computing*, WINDOWS, http://tinyurl.com/ke4rtty (last visited May 8, 2015).

- **Encrypt data before loading it into the cloud.** A number of tools can encrypt data before transmitting it to the cloud. Two popular ones are Boxcryptor and MEO File Encryption Software. Boxcryptor advertises that it can securely encrypt files before they are uploaded to the cloud, and this service works with Dropbox, Google Drive, Microsoft OneDrive, SugarSync, Box.com and any other major cloud storage provider. MEO File Encryption Software offers a similar process, but can also assist in sending encrypted e-mails; it allows customers to use encrypted e-mail even if the receivers do not have the decrypting software on their machines.

- **Limit access to cloud storage files.** Only those who need access to files in the cloud storage account should be authorized to access them. Once they no longer need that access, it should be immediately terminated. Moreover, although a defense team member may need to review information in a certain folder, he or she need not be given access to the entire account.

- **Receive and review records of access to your data.** Most cloud companies will provide periodic reports of who has accessed your data. Reviewing this for any improper access will improve your security.
Security trumps convenience when selecting service options. Some popular cloud services may impair your security. They frequently offer “helpful” applications such as automatically transferring information from devices to the cloud or vice versa when accessing the service (this is a popular feature with Dropbox). As enticing as that service may be, users should change it so that the cloud provider only automatically transfers those files that the customer wants to transfer. Bear in mind that some cloud services provide these options as their default setting, requiring manual override to change them.

Other things to avoid, so as to keep account security primary, include:

- “Log off” the service when finished, do not just “exit” from it.
- Do not select “remember me” on your devices when accessing the cloud, as it also allows others to log in to the service as you without your password.
- Enable automated notifications of account activity, sending e-mail alerts when a password reset is requested for your account.

Create strong passwords. Cybersecurity experts currently recommend using a 12-character password. Passwords with fewer characters are more susceptible to being hacked. Also consider using full sentences (such as “Mybeaglerescuedme!”) or passphrases (such as “Courthouseterror?!”) that are both easier to remember and harder to hack. Adding non-letter characters (a number or a symbol) will make it even more difficult for hackers to access your password.

Consider implementing two-factor authentication. Two-factor authentication is becoming a popular way to substantially increase the security of cloud storage. It uses “something you know” (like a password) and “something you have” (like a phone). Commonly, cloud storage services implement two-factor authentication by sending a second code to customers’ telephones after they enter their password. Only after entering the second code that was sent to the phone will the service permit access to their account. Many cloud computing services now allow the use of two-factor authentication. For instance, Duo for Cloud offers to integrate two-factor authentication with existing Google Apps, Box.com, Office 365, OneLogin, Amazon Web Services, and Salesforce applications. (See Cloud Authentication for Apps, DUO SECURITY, http://tinyurl.com/ma86nds (last visited May 8, 2015).)

Consider using biometrics for cloud access security. Alternatively, another means of substantially increasing security of cloud storage is using biometric “passwords” in order to access data. This is a growing popular means of controlling access to cloud data. Common biometric examples include fingerprint, voice or facial recognition, or an eye scan. For better security, biometrics (such as a fingerprint) combined with a password produce a highly secure two-factor authentication option.

Human error remains the weakest link. People, through our own human failings, laziness, and ignorance, can create the greatest security risks to cloud data. Data breaches that have occurred due to lost flash drives, smartphones, or laptops (that were not encrypted) can become exponentially worse when those devices link to massive data in the cloud. Smartphones are particularly vulnerable given that they are easily lost and too often have no password protection at all. From using weak passwords, to being tricked into providing a spoofed “friend” access, to allowing viruses and malware to get onto the system, to leaving an iPhone at Starbucks—remember that it is human error that often compromises the security of cloud information.
Conclusion
Cloud options provide a great opportunity to increase efficiency, quickly share information, and improve productivity. But it is imperative for attorneys to have a basic working knowledge of technological advances and unintended risks that these advances can have with client information in the cloud. By understanding how relevant technology like cloud computing works, solo and small firm practitioners can utilize these tools to keep up with their clients’ needs as well as the standard of care for modern criminal defense. Ideally, small firms will periodically invest in an IT consultant to ensure the most competent use of cloud technology as well as the greatest security of confidential information placed in the cloud. But even without that, following the recommendations presented above will dramatically reduce the risks of using cloud computing.

DONNA LEE ELM is the federal defender for the Middle District of Florida, practicing in Tampa. She is the defender member on a joint working group with DOJ that produced the criminal e-discovery protocol, serves on the Defender Automation Working Group, and can be reached at donna_elm@fd.org. SEAN BRODERICK is the national litigation support administrator for the Defender Services Office in Oakland, California. He provides guidance and recommendations to courts, federal defender offices, and court-appointed attorneys in federal criminal cases on e-discovery and complex cases, and can be reached at sean_broderick@fd.org.
United States v. [Defendant]
[Case No.]
Discovery Production Log
(Most Recent Revised Date)

<table>
<thead>
<tr>
<th>Receipt Date</th>
<th>Bates</th>
<th>Description (broad, including cover letter info)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Initial Discovery Assessment Checklist

In cases involving large volumes of data in a variety of media and/or file formats produced as part of the discovery, the trial team should contact the National Litigation Support team and together try to answer the questions below. The answers will direct the work flow and assist the trial team in further planning their strategy and budget.

1. Is there any way to estimate the total volume of the discovery production even though some of it may come later?
2. Will we be able to access all the data?
3. Is any of the data encrypted?
4. Are there specific types of documents that will be irrelevant to our case? (i.e. pictures, executable files, junk emails, etc.)
5. Are there specific types of documents that will be very important to our case? (i.e. emails authored by a particular person, documents created during a specific time period, specific document types such as bank records, etc.)
6. Are there both paper documents that have been scanned and native electronic files?
7. Should we objectively code the scanned documents so that they can be integrated into the native file data set for purposes of searching and organization?
8. Will there continue to be rolling discovery productions?
9. Do we need to look at the entire production?
10. Will the documents need to be shared among the Federal Defender Office, CJA Panel Attorneys and Retained Counsel?
11. Does the trial team already have an Evidence Review Platform in their office that could handle the amount and variety of discovery involved?
12. What is the timeline for completing the review?
Cellebrite Reader Request Language

**Request For Cellebrite Data.** Upon a defendant's request, the government must permit a defendant to inspect and to copy or photograph the results or reports of any physical or mental examination and of any scientific test or experiment if:

(i) the item is within the government's possession, custody, or control;

(ii) the attorney for the government knows--or through due diligence could know--that the item exists; and

(iii) the item is material to preparing the defense or the government intends to use the item in its case-in-chief at trial.

Fed.R.Crim.Pro. 16(F).

It is counsel’s understanding that government agents used a forensic tool called Cellebrite UFED to extract data from a digital device. Generally, there are three types of extractions that can be performed: logical, file system, and physical. Once data has been extracted, the government has several options on how to produce the data to the defense. When data is extracted from a digital device, the data can be stored in several formats depending on the type of device and type of extraction. After many extractions, Cellebrite saves a report of the data in .html (the “original .html version”). Additionally, a file is created with .ufd or .ufdx extensions. Moreover, depending on the extraction type, other data may be stored in .bin; ZIP/TAR extensions. As for the .ufd and .ufdx file formats, Cellebrite allows license holders to send a free reader which allows others to view the files in original file format (the .UFDR file format).

Accordingly, pursuant to Fed.R.Crim.Pro. 16(F), Mr. XXX moves this Court to order the government to produce the following for each extraction completed on each digital device:

(1) The original .html version of the report;
(2) The UFED Reader;
(3) The UFDR report; and
(4) All data captured as a result of the extraction (e.g., .bin files; ZIP/TAR files; etc.).
Jurisdictions with Pretrial Conference Guidelines

The following jurisdictions either require or allow a pretrial conference to discuss discovery, and have guidelines for either what should be addressed at a pretrial conference or what should be included in a joint written statement memorializing such a conference:

1. California, Northern District
2. Illinois, Northern District
3. Massachusetts
4. Nevada
5. New Jersey
6. Northern Mariana Islands
7. Oklahoma, Western District
8. Puerto Rico
9. West Virginia, Northern District
1. California, Northern District

17.1-1. Pretrial Conference

(a) Time for Pretrial Conference. On request of any party or on the Judge's own motion, the assigned Judge may hold one or more pretrial conferences in any criminal action or proceeding.

(b) Pretrial Conference Statement. Unless otherwise ordered, not less than 7 days prior to the pretrial conference, the parties shall file a pretrial conference statement addressing the matters set forth below, if pertinent to the case:

1. Disclosure and contemplated use of statements or reports of witnesses under the Jencks Act, 18 U.S.C. § 3500, or Fed. R. Crim. P. 26.2;

2. Disclosure and contemplated use of grand jury testimony of witnesses intended to be called at the trial;

3. Disclosure of exculpatory or other evidence favorable to the defendant on the issue of guilt or punishment;

4. Stipulation of facts which may be deemed proved at the trial without further proof by either party and limitation of witnesses;

5. Appointment by the Court of interpreters under Fed. R. Crim. P. 28;

6. Dismissal of counts and elimination from the case of certain issues, e.g., insanity, alibi and statute of limitations;

7. Joinder pursuant to Fed. R. Crim. P. 13 or the severance of trial as to any codefendant;

8. Identification of informers, use of lineup or other identification evidence and evidence of prior convictions of defendant or any witness, etc.;

9. Pretrial exchange of lists of witnesses intended to be called in person or by deposition to testify at trial, except those who may be called only for impeachment or rebuttal;

10. Pretrial exchange of documents, exhibits, summaries, schedules, models or diagrams intended to be offered or used at trial, except materials that may be used only for impeachment or rebuttal;

11. Pretrial resolution of objections to exhibits or testimony to be offered at trial;

12. Preparation of trial briefs on controverted points of law likely to arise at trial;

13. Scheduling of the trial and of witnesses;

14. Request to submit questionnaire for prospective jurors pursuant to Crim. L.R. 24-1, voir dire questions, exercise of peremptory and cause challenges and jury instructions;
(15) Any other matter which may tend to promote a fair and expeditious trial.

2. Illinois, Northern District

LCrR16.1. Pretrial Discovery and Inspection
(a) Discovery Conference. Within 7 days after the arraignment the United States attorney and the defendant’s attorney shall confer and attempt to agree on a timetable and procedures for the following:

(1) inspecting, copying, or photographing any of the information subject to disclosure pursuant to Fed.R.Crim.P. 16;

(2) preserving the written notes of government agents;

(3) identification and notification of evidence the United States attorney intends to introduce pursuant to Federal Rule of Evidence 404(b);

(4) the filing of a proffer made within the scope of U.S. v. Santiago, 582 F.2d 1128 (7th Circ., 1978);

(5) the filing of materials subject to 18 U.S.C. §3500; and

(6) any other preliminary matters where such agreement would serve to expedite the orderly trial of the case.
RULE 116.5 STATUS CONFERENCES AND STATUS REPORTS PROCEDURE

(a) Initial Status Conference. On or about the 14th day following the date scheduled for the completion of automatic discovery, the Magistrate Judge shall convene an Initial Status Conference with the attorneys for the parties who will conduct the trial. Unless otherwise ordered by the court, counsel shall confer and file a joint memorandum no later than 7 days before the Initial Status Conference. The joint memorandum must include the following issues and any other issues relevant to the progress of the case, which counsel must be prepared to discuss at the conference:

1. the status of automatic discovery and any pending discovery requests;
2. the timing of any additional discovery to be produced;
3. the timing of any additional discovery requests;
4. whether any protective orders addressing the disclosure or dissemination of sensitive information concerning victims, witnesses, defendants, or law enforcement sources or techniques may be appropriate;
5. the timing of any pretrial motions under Fed. R. Crim. P. 12(b);
6. the timing of expert witness disclosures;
7. periods of excludable delay under the Speedy Trial Act;
8. the timing of an Interim Status Conference or Final Status Conference, as the case may require.

(b) Interim Status Conference. At the Initial Status Conference, unless the Magistrate Judge decides to transfer the case to the District Judge under subsection (a) of this rule, the Magistrate Judge shall schedule an Interim Status Conference or a Final Status Conference, as needed, giving due regard to the complexity of the case and the period of time that the parties expect will be required to complete discovery and pretrial motions. Unless otherwise ordered by the court, counsel shall confer and file a joint memorandum no later than 7 days before the Interim Status Conference. The joint memorandum must address the following issues, and any other issues relevant to the progress of the case, which counsel must be prepared to discuss at the conference:

1. the status of automatic discovery and any pending discovery requests;
2. the timing of any additional discovery to be produced;
3. the timing of any additional discovery requests;
4. whether any protective orders addressing the disclosure or dissemination of sensitive information concerning victims, witnesses, defendants, or law enforcement sources or techniques may be appropriate;
5. the status of any pretrial motions under Fed. R. Crim. P. 12(b);
6. the timing of expert witness disclosures;
7. defenses of insanity, public authority, or alibi;
8. periods of excludable delay under the Speedy Trial Act;
9. the status of any plea discussions and likelihood and estimated length of trial;
10. the timing of the Final Status Conference or any further Interim Status Conference.

…
(b) **Final Status Conference.** In all felony cases and Class A misdemeanor cases to be heard by a District Judge, before the Magistrate Judge issues the Final Status Report required by subdivision (d) of this rule, the Magistrate Judge shall, if necessary, convene a Final Status Conference with the attorneys who will conduct the trial. Counsel shall confer and file a joint memorandum no later than 7 days before the Final Status Conference. The joint memorandum must address the following issues, and any other issues relevant to the progress of the case, which counsel must be prepared to discuss at the conference:

1. whether the defendant requests that the case be transferred to the District Judge for a Rule 11 hearing;
2. whether, alternatively, the parties move for a pretrial conference before the District Judge in order to resolve pretrial motions (if any) and schedule a trial date and, if so:
   - whether the parties have produced all discovery they intend to produce and, if not, the identity of any additional discovery and its expected production date;
   - whether all discovery requests and motions have been made and resolved and, if not, the nature of the outstanding requests or motions and the date they are expected to be resolved;
   - whether all motions under Fed. R. Crim. P. 12(b) have been filed and responded to and, if not, the motions that are expected to be filed and the date they will ready for resolution;
   - whether the Court should order any additional periods of excludable delay, the number of non-excludable days remaining, and whether any matter is currently tolling the running of the time period under the Speedy Trial Act; and
   - the estimated number of trial days; and
3. any other matters specific to the particular case that would assist the District Judge upon transfer of the case from the Magistrate Judge.
4. Nevada

LCR 16-1

(a) Complex Cases.

(2) In all cases designated as complex, the parties shall, not later than seven (7) days following such designation, confer to develop a proposed complex case schedule, addressing the following:

(A) The scope, timing, and method of the disclosures required by federal statute, rule, or the United States Constitution, and any additional disclosures that will be made by the government;

(B) Whether the disclosures should be conducted in phases, and the timing of such disclosures;

(C) Discovery issues and other matters about which the parties agree or disagree, and the anticipated need, if any, for motion practice to resolve discovery disputes;

(D) Proposed dates for the filing of pretrial motions and for trial; and,

(E) Stipulations with regard to the exclusion of time for speedy trial purposes under Title 18, U.S.C. § 3161.

...

(b) Non-Complex Cases. In cases which are not designated as complex under section 16-1(a), the parties shall confer to designate whether discovery in the case will be governed by a joint discovery agreement or a government disclosure statement.

(2) Government Disclosure Statement.

(A) In cases in which the parties have not entered into a joint discovery agreement, the government shall file a disclosure statement. In such cases, within seven (7) days of arraignment, the parties shall confer regarding the timing, scope, and method of the disclosures and reciprocal disclosures required by federal statute, rule, or the United States Constitution, and any additional disclosures which will be made by the government.

(B) Within seven (7) days of the conference, but in no event more than fourteen (14) days after the date of arraignment, the government shall file its disclosure statement, which shall include the following information:

   (i) The date on which the parties discussed the disclosure statement, or an explanation of why a discussion has not occurred;

   (ii) The scope, timing, and method of the government’s disclosures required by federal statute, rule or the United States Constitution; and,

   (iii) The scope, timing, and method of any additional disclosures which will be made by the government.
5. New Jersey

*Standing Order 15-2: In Re Criminal trial Scheduling and Discovery: “…it is the judgement of this Court that such a protocol for trial scheduling and discovery should be implemented for all felony cases in the District of New Jersey that are initiated on or after April 1, 2016.”

Requires parties to meet before arraignment and decide on schedule for initial exchange of discovery. The scheduling order linked below details the types of evidence and on what dates disclosure was agreed upon.

EXHIBIT 2: [Link at p. 9–11] Scheduling order for criminal cases requiring extensive discovery

This matter having come before the Court for arraignment; and the United States being represented by Paul J. Fishman, United States Attorney for the District of New Jersey (by ____________________, Assistant U.S. Attorney, appearing); and the Defendant being represented by ____________________; and the parties having met and conferred prior to arraignment and having determined that this matter may be treated as a criminal case that requires extensive discovery within the meaning of paragraph 4 of this Court’s Standing Order for Criminal Trial Scheduling and Discovery; and the parties having agreed on a schedule for the initial exchange of discovery; and the Court having accepted such schedule, and for good cause shown,

It is on this ___ day of ___, 20__, ORDERED that:

1. The Government shall provide any oral, written or recorded statement of the Defendant or, in the case of an organizational defendant, of any person who is legally able to bind the Defendant because of that person’s position as a director, officer, employee or agent of the Defendant on or before ________________________.

2. The Government shall provide exculpatory evidence, within the meaning of Brady v. Maryland, 373 U.S. 83 (1963) and its progeny, on or before ________________________,. Exculpatory evidence that becomes known to the Government after that date shall be disclosed reasonably promptly after becoming known to the Government.

3. If there is more than one defendant named in the indictment, and if the Government intends to introduce into evidence in its case-in-chief a confession made to law enforcement authorities by one defendant that names or makes mention of a co-defendant, a copy of that statement or confession shall be disclosed by the Government on or before ________________________. The Government shall provide a proposed redaction to that statement to conform with the requirements of Bruton v. United States, 391 U.S. 123 (1968) and its progeny, on or before ____________________________.

4. [The parties should make a good faith attempt to establish a reasonable schedule for the remainder of discovery required by Federal Rule of Criminal Procedure 16(a)(1), and to set forth that schedule in this paragraph.]
5. The defendant shall provide any and all notices required by Federal Rules of Criminal Procedure 12.1, 12.2, and 12.3 on or before __________________________. 6. [The parties should make a good faith attempt to establish a reasonable schedule for the remainder of discovery required by Federal Rule of Criminal Procedure 16(b)(1), and to set forth that schedule in this paragraph.]

7. A status conference shall be held on __________, at _______ a.m./p.m., in order to assess the progress of discovery; to determine a schedule for the production of additional discovery if necessary; to consider any discovery disputes if necessary; to set or consider setting a schedule for the next status conference in this matter; and to set or consider setting a schedule for pretrial motions if a date for the completion of discovery can be determined.

EXHIBIT 3: [Link at p. 12–13] Scheduling order for cases where parties could not determine a schedule for discovery exchange
6. Northern Mariana Islands

LCrR 17.1.1 - Pretrial Conference.
On request of any party or on the court’s motion, one or more pretrial conferences may be held. The agenda shall consist of the following items, so far as applicable:
   a. Production of statements or reports of witnesses under the Jencks Act, 18 U.S.C. §3500;
   b. Production of grand jury testimony of witnesses intended to be called at the trial;
   c. Production of evidence favorable to the defendant on the issue of guilt or punishment as required by Brady v. Maryland, 373 U.S. 83 (1963), and related authorities;
   d. Stipulation of facts which may be deemed proved at the trial;
   e. Appointment of interpreters under Fed.R.Crim.P. 28;
   f. Dismissal of certain counts and elimination of certain issues, e.g., insanity, liability, and statute of limitations;
   g. Severance of the trial of any co-defendant or joinder of any related case;
   h. Use or identification of an informant, use of lineup or other identification evidence, use of evidence of prior convictions of defendant or any witness;
   i. Pretrial exchange of lists of witnesses, expert or other, intended to be called in person or by deposition to testify at trial, except those who may be called for the only for impeachment or rebuttal;
   j. Pretrial resolution of objections to exhibits or testimony to be offered at trial;
   k. Preparation of trial briefs on legal issues likely to arise at trial;
   l. Scheduling of the trial and the order of witnesses; m. Discussion of proposed jury instructions and voir dire jury examination.
LCrR16.1 Discovery Conference.

(b) Joint Statement. Within 7 days following completion of the required discovery conference, the parties shall file a joint statement memorializing the discovery conference. (The Joint Statement of Discovery Conference shall conform to the form provided herein as Appendix V.)

Joint Statement of Discovery Conference Referenced in LCrR16.1(b)

This joint statement is submitted pursuant to LCrR16.1(b).

1. Date Conference Held: ___________________, within 14 days of the appearance before Magistrate Judge where a plea of not guilty was entered.

2. Names of the attorneys who attended the conference:
   U.S. Attorney/AUSA__________________________________________________________
   Defense Attorney__________________________________________________________
   Retained _____; Appointed: _____
   Federal Public Defender/Assistant FPD _____ or Panel Member ______

Counsel met for purposes of exchanging discovery materials in accordance with the Federal Rules of Criminal Procedure as supplemented by the Local Criminal Court Rules and any orders of this court and, as a result of the conference, the undersigned counsel report the following:

3. The specific time, date and place at which the offense(s) charged is/are alleged to have been committed:

4. (a)(1) Any contested issues of discovery and inspection raised by counsel for plaintiff: Appx.V - 1
   (2) Any contested issues of discovery and inspection raised by counsel for defendant:
   (b) Any additional discovery or inspection desired by either party:

5. The fact of disclosure of all materials favorable to the defendant or the absence thereof within the meaning of Brady v. Maryland and related cases: Counsel for plaintiff expressly acknowledges continuing responsibility to disclose any material favorable to defendant within the meaning of Brady that becomes known to the Government during the course of these proceedings.

6. The fact of disclosure of the existence or nonexistence of any evidence obtained through electronic surveillance or wiretap:

7. The fact of disclosure of the contemplated use of the testimony of an informer. (Include only the fact an informer exists and not the name or testimony thereof):
8. The fact of disclosure of the general nature of any evidence of other crimes, wrongs, or acts the government intends to introduce at trial pursuant to Fed. R. Evid. 404(b):

9. The fact of disclosure of the prior felony convictions of any witness the government intends to call in its case-in-chief:

10. The resolution, if any, of foundational objections to documentary evidence to be used by both parties (except for the purpose of impeachment):

11. The resolution, if any, of chain-of-custody matters (where at issue):

12. The resolution, if any, of the admissibility of any reports containing scientific analysis without requiring the expert’s attendance at trial:

13. The parties will provide each other with the opportunity to inspect any demonstrative evidence, representational exhibits or charts.

Counsel for both parties state that presently there are no additional matters of discovery presently known.

Counsel expressly acknowledges the obligation to produce these item(s) as soon as practicable, but in no event later than 14 days prior to the trial of this cause. Counsel also expressly acknowledges continuing obligation to disclose any materials that become known to counsel during the course of the pretrial investigation of this cause.

14. Notice of Alibi:

15. Notice of Insanity Defense or Expert Testimony of Defendant’s Mental Condition:

16. Notice of Defense Based on Public Authority:

At the conclusion of this conference, counsel conferred concerning the contents of this joint statement.
8. Puerto Rico

RULE 117.1 STATUS AND PRETRIAL CONFERENCES

(a) At earliest practical time before trial consistent with Speedy Trial Act, Court may conduct initial status conference. Court may at any time schedule additional status conferences.

(b) Matters to Discuss at Pretrial Conferences. The trial or leading attorneys shall appear prepared to:

1. Discuss any discovery or other motions that have been filed by any party and await the Court’s ruling, including, if necessary, the scheduling of any motion to dismiss, suppress or sever;
2. discuss any matter known to counsel that may cause a delay or continuance of the trial, including the waiver of jury trial;
3. discuss the establishment of a reliable trial date and the probable length of trial, unless the Court has issued a Scheduling Order;
4. establish a schedule for the filing and briefing of possible motions in limine, proposed voir dire questions, jury instructions and, if appropriate, trial briefs;
5. discuss the number of witnesses and their availability for the trial;
6. discuss and enter into stipulations to undisputed facts and/or testimony of an absent witness;
7. discuss the exclusion from admissible statements of materials which may be prejudicial to codefendants;
8. discuss any special trial arrangements, including seating, security measures, necessity for sequestration of the jury, potential witnesses outside courthouse environs, and any other matter which may facilitate or expedite the trial;
9. discuss the number and use of peremptory challenges;
10. discuss the procedures on objections, the order of cross-examination, and the order of presentation of evidence and argument, where there are multiple defendants;
11. any other aspect or matter of the case. Any co-counsel or attorney who, by exception, is allowed to substitute for the trial attorney must also comply with the requirements of subsection (b)(1) through (b)(11).
(2) In all cases designated as complex, the parties shall, not later than seven (7) days following such designation, confer to develop a Proposed Complex Case Schedule addressing the following:

(i) the scope, timing, and method of the disclosures required by federal statute, rule, or the United States Constitution, and any additional disclosures that will be made by the government;

(ii) whether the disclosures should be conducted in phases, and the timing of such disclosures;

(iii) discovery issues and other matters about which the parties agree or disagree, and the anticipated need, if any, for motion practice to resolve discovery disputes;

(iv) proposed dates for the filing of pretrial motions; and

(v) stipulations with regard to the exclusion of time for speedy trial purposes under 18 U.S.C. § 3161.
UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, 

Plaintiff,

vs.

[LEAD DEFENDANT], et al

Defendants.

Case No.:

COMPLEX CASE MANAGEMENT ORDER

A. INITIAL MEET AND CONFER: By not later than [date 7 calendar days after Post-Indictment Arraignment], prior to the USAO’s filing of the First Status Report (see Section C, infra), the United States Attorney’s Office (“USAO”) shall meet and confer with counsel for all defendants and individuals with sufficient technical knowledge and experience regarding electronically stored information (“ESI”), to reach agreement on the format and mode of transmission of ESI discovery, including:

Complex Case Management Order
a. Production of ESI, under each of the general categories discussed in Section 6(i), infra, in a searchable, reasonably usable, cross platform or open platform format (i.e. searchable PDF format, TIFF and OCR format, Native files as received, Native files with metadata, etc.);

b. Case mapping, indexing, and organizational software generally used by, and available to, the USAO and defense counsel;

c. The practicability of sharing indexed or organized ESI without revealing work product;

d. Production of ESI received from third parties in a reasonably usable, cross platform or open platform format that conforms to industry standards;

e. Confidential, private, or sensitive information in any ESI discovery that will be produced, and:

i. how recipients will prevent unauthorized access to, or disclosure of, such ESI discovery to unauthorized parties;

ii. the need for the producing party to seek a protective order from the court addressing the management of the particular ESI at issue;

iii. whether redaction or encryption is warranted;

iv. what steps will be taken at the conclusion of the case to return confidential or sensitive discovery to the producing party.

f. Proprietary or legacy data (e.g., video surveillance recordings in an uncommon format, proprietary databases, or software that is no longer supported by the vendor) and suitable generic output form,
or specific requirements necessary to access data in its original format;

g. Attorney-client or protected information issues, including methods or procedures for segregating such information and resolving disputes;

h. Naming conventions (e.g., in a Title III wire tap case naming conventions should be established for audio files, monitoring logs, and call transcripts, to facilitate cross-referencing the audio calls with the corresponding monitoring logs and transcripts);

i. Software or hardware limitations of the USAO or defense counsel;

j. Issues specific to ESI produced from a seized or searched third-party digital device, such as identifying the device’s probable owner or custodian and the need for a protective order to regulate the receiving party’s access to or inspection of the device;

k. Inspection of hard drives and/or forensic (mirror) images, where specialized software is required to access the stored information;

l. Access to already extracted metadata from third party ESI in an industry standard load file format;

n. Appointment of a Coordinating Discovery Attorney (“CDA”) (see Section F, infra).

B. **FIRST STATUS CONFERENCE:** All parties and their counsel shall appear for an initial status conference in this matter on [date 21 calendar days after Post-Indictment Arraignment].

C. **FIRST STATUS REPORT OF GOVERNMENT:** By not later than [date 14 calendar days after Post-Indictment Arraignment], following the Initial Meet and Confer with defense counsel, (see Section A, supra), the USAO shall file a document entitled “First Status Report.” For good cause shown, the USAO may file portions of the First Status Report in camera and/or under seal. The First Status Report shall:

Complex Case Management Order
1. For each defendant who has not yet made an appearance in this case, specify:
   a. Why the defendant has not yet made an appearance;
   b. When the defendant is expected to make an appearance, if this is known or can be reasonably estimated;
   c. Any factors that make it difficult to reasonably estimate when the defendant will make an appearance; and,
   d. For any defendant already in state or federal custody on other charges:
      i. Whether the charges underlying the custody are related to the charges in this case and, if so, how; and,
      ii. Whether the charges underlying the custody have been or will be resolved before the defendant makes an appearance in this case.

2. For each defendant who has made an appearance in this case:
   a. Specify whether the defendant has been detained or granted bond and, if detained, provide the registration number;
   b. Specify whether the defendant is believed to require an interpreter, and if so, the language;
   c. Specify whether the defendant is currently known to have a medical or mental condition that warrants special attention, treatment, or accommodation; and,
   d. If the defendant has been detained or remained in custody due to a failure to satisfy bond conditions confirm that the defendant’s counsel has been advised of the institution in which the defendant is currently being held. (The USAO shall also file separately with the court, under seal and in...
camera, a list of in-custody defendants that identifies the
institution in which each in-custody defendant is being held.)

3. Include as attachments each of the charts specified under (C) below.

4. State whether the USAO currently plans to seek additional charges related
to this case, and if so, when (this portion of the First Status Report
may be filed in camera and under seal if the USAO has concerns
that revealing planned additional charges might cause potential
targets to flee or jeopardize an ongoing investigation).

5. Estimate the following with respect to trial, assuming that all defendants
named in the pending indictment were to make appearances and
proceed to trial (such estimate not to be binding on the USAO):

a. Number of government witnesses; and

b. Number of trial days for the government’s case-in-chief (assuming
   reasonable cross-examination).

6. Estimate the following with respect to discovery, assuming that all
defendants named in the pending indictment were to make
appearances and proceed to trial (such estimate not to be binding on
the USAO):

a. With respect to search warrants:
   i. Number of warrants;
   ii. Number of locations searched;
   iii. Pages of documents seized;
   iv. Number of digital devices seized;
   v. Number and general description of items of physical evidence
      seized.

b. With respect to wiretaps:
   i. Number of applications;
ii. Number of target telephones;

iii. Hours of audio recordings, specifying hours in English and, if applicable, hours in foreign languages and which languages;

iv. Pages of transcripts.

c. With respect to other audio- or video-recordings:

i. Hours of recordings, specifying hours in English and, if applicable, hours in foreign languages and which languages;

ii. Pages of transcripts.

d. With respect to physical evidence, including photographs:

i. Number of items;

ii. General description of items;

iii. Number and, if known, identity of locations at which items will be made available for inspection.

e. With respect to digital devices:

i. Number and kind of devices seized or otherwise obtained;

ii. Whether originals and/or forensic images have been retained, returned, or destroyed;

iii. Whether government will make originals and/or forensic images available;

iv. Number of pages of documents printed or otherwise stored by the government from data obtained from each device.

f. With respect to confidential informants anticipated to provide testimony at trial:

i. Number of such informants;

ii. Hours of audio- or video-recordings;
iii. Pages of transcripts;

iv. Pages of other documents (e.g., criminal histories, payment histories, interview reports).

g. With respect to foreign evidence:

i. Countries of origin;

ii. Nature and type, including whether in foreign languages and which languages;

iii. Hours of audio- or video-recordings;

iv. Pages of transcripts;

v. Pages of other documents;

vi. Whether any foreign evidence requests remain pending, and if so, a general description of the evidence sought.

h. With respect to written discovery (excluding items covered by more-specific sub-categories above), number of pages for the following:

i. Law enforcement agent reports;

ii. Expert reports (e.g., chemist reports or other reports of scientific analyses);

iii. Transcripts (e.g., grand jury or other court-proceedings);

iv. Business records (e.g., bank records, toll records, pen register records, correspondence, emails).

i. With respect to ESI (including electronically stored written discovery), the nature (i.e. file format), volume, and mechanics of producing the following categories of ESI, as agreed upon during the Initial Meet and Confer (see Section A, supra):
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. Acquired 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.

7. Propose a schedule for completion of discovery (assuming production under the terms set forth under (D) below), and identify for the court any types of discovery as to which the need to limit disclosure (e.g., child pornography, trade secrets, malware, personal identifying information) may require limits on one or more defendant’s access to discovery that cannot be accomplished by redaction.

8. Provide any other information that may assist the court, the USAO, or the defense in handling this matter efficiently and cost-effectively.

D. CHARTS

1. As specified in (B)(3) above, the government’s First Status Report shall have as attachments each of the following summary charts (which shall also be provided to chambers email in Word or Word Perfect format:

   a. A table of contents to the indictment;

   b. A chart listing the defendants charged in each count of the indictment, arranged by count number;

   c. A chart listing the defendants and the respective counts with which they have been charged, arranged alphabetically by last name of the defendant, and listing the predicate acts/overt acts alleged as to a particular defendant for any RICO/conspiracy counts;

   d. The chart described in the previous subparagraph, arranged by defendant’s position in the caption of the indictment;
e. A chart grouping and identifying those defendants who are blood relatives or relatives by marriage (common law or otherwise), if known, and specifying the relationship; and,
f. A chart addressing relative culpability by placing each defendant in one of the following four categories: (1) most culpable; (2) next-most culpable; (3) next-to-least most culpable; (4) least culpable. These designations shall be based only on conduct alleged in the indictment, shall not be affected by prior criminal convictions or cooperation with the USAO, and shall not be binding on the USAO, meaning that USAO may change its position regarding relative culpability at any time, including during plea negotiations, at trial, or at sentencing.

2. On each of the above summary charts, next to the name of each defendant the USAO shall add, in parentheses, the name of that defendant’s attorney.

3. Within 7 calendar days after the filing of any superseding or otherwise new or redacted indictment in this case, the USAO shall file modified summary charts to reflect allegations in any superseding or otherwise new or redacted indictment.

E. DISCOVERY: The USAO shall produce discovery, whether to a CDA (see Section F, infra) or an individual attorney or pro se defendant, as follows:

1. Master Discovery Index: With each production of discovery, the USAO shall provide to the CDA and any individual attorney or pro se defendant not receiving discovery through the CDA, a master index of all discovery produced in this case, updated to reflect the current production. This master index shall identify discovery as follows:
a. Written discovery shall be identified by Bates number range, with
document(s) within each range identified by general type
(e.g., interview reports, wire tap transcripts, business records,
search warrant or wiretap applications).

b. ESI discovery shall be identified by general category (e.g., digital
device forensic image, investigation reports, surveillance
footage, etc.), location (e.g., CD, DVD, Thumb Drive, Hard
Drive), source (e.g., wiretap, third-party subpoena, seizure),
and, where applicable, format (e.g., TIFF, PDF). For ESI
that is generated by the government, the government will
make its best efforts to use a consistent file naming
convention that will make it easy to cross-reference related
ESI. For example, in a Title III wire tap case the government
will make its best efforts to use a consistent file naming
convention for the audio files, monitoring logs, call
transcripts, and other similar items, so that the files can
easily be cross-referenced.

c. Audio or video recordings shall be identified by date of recording,
source (e.g., target telephone intercepted, location of
recording), and, to the extent possible, participants. The
USAO’s identification of participants in the master discovery
index shall not be binding on the USAO.

d. Physical evidence shall be identified by type (e.g., narcotics,
weapons), quantity or number (e.g., kilos of cocaine, number
of pills, number of weapons), date and manner by which
obtained (e.g., seized pursuant to search warrant issued on
particular date and executed on particular date), and current
2. **Draft Transcripts**: At the same time as it files its First Status Report, the government shall file an agreement to be executed by defendants and their counsel stipulating that draft transcripts of recorded calls or recorded surveillance may not be used for cross-examination or other purposes and may not be distributed to any defendant or counsel who have not executed the agreement, unless otherwise ordered by the court. If draft transcripts are prepared, the USAO: (a) will make them available to all counsel and pro se defendants who have executed the agreement, pursuant to all terms of the agreement, including the terms regarding non-distribution; and (b) if a CDA is appointed, will make them available to the CDA, who will distribute them to those counsel appointed to represent a defendant under the Criminal Justice Act (“CJA Defense Counsel”), the Federal Public Defender’s Office (“FPDO”), provided that the FPDO has opted to utilize the services of the CDA, and pro se defendants who have executed the agreement, pursuant to all terms of the agreement, including the terms regarding non-distribution.

3. **Discovery From Investigating Agencies**: The USAO shall provide to a responsible representative of each law enforcement agency -- local, state, or federal, including penal institutions -- in possession of potentially discoverable material, including possible *Brady* and *Henthorn* material, specific instructions regarding the nature of such discoverable material under federal law and the type of search that must be accomplished to locate and identify such discoverable material and custodian (e.g., FBI evidence locker with identification of responsible agent).
material. As part of its Second Status Report (discussed in Section J below), the USAO shall confirm that such instructions have been given and list the representatives receiving the instructions.

4. **Discovery Format:** To the extent possible, the USAO will produce discovery in a searchable, reasonably usable, cross platform or open platform format using the following standard format conventions, and, if it is able to do so, shall not be required to produce discovery in any other format, regardless of any requests by individual defense counsel:

a. Written discovery may be produced in that form, made available for inspection, or produced as electronic files that can be viewed and searched, using one of the following methods:
   
   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, sequential 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, sequential 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 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, sequential Bates number.

b. ESI discovery shall be produced using one of the following
methods:

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, sequential Bates number. (2) Text
from that original document is extracted or pulled out and
stored without formatting in a generic format. (3) Metadata
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 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.

c.  ESI discovery 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), shall identify the digital device that held the ESI, indicate the device’s probable owner or custodian, and indicate the location where the device was seized or searched.  Where the USAO has limited authority to search the digital device (e.g., limits set by a search warrant’s terms), the USAO shall confer with defense counsel to discuss the need for a protective order or other mechanism to delineate defense counsel’s access to, or inspection of, the device.  The USAO will maintain the originals of all electronic files it has authority to retain, whether obtained from acquired digital devices or by other means.  If retention has been authorized, the USAO will maintain the originals and/or original forensic images of all
acquired digital devices. The USAO will produce a copy of any such forensic image along with instructions that will enable the extraction and reading of files contained on any such forensic image.

d. ESI discovery received from third parties should be produced in the format it was received or in a reasonably usable, cross platform or open platform format. The USAO shall retain a copy of the ESI as it was originally produced, in the event that the copy is subsequently needed to perform quality control or verification of the discovery produced.

e. Photographs and video and audio recordings that either were originally created using digital devices or have previously been digitized should be produced as digital copies of the images or recordings, if they are in the USAO’s possession, custody or control. 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 USAO is not required to convert materials obtained in analog format to digital format for discovery.

f. ESI discovery should be transmitted on electronic media of sufficient size to hold the entire production (e.g., a CD, DVD, or thumb drive). If the size of the production warrants a large capacity hard drive, the USAO will, upon request, make discovery available on external, stand alone hard drives, which hard drives must be provided to the USAO by
defense counsel and must meet requirements to be specified by the USAO.

g. Discovery shall be clearly labeled with the case name and number, a unique identifier for the electronic media (e.g., a CD, DVD, or thumb drive), and the production date. A cover letter should accompany each transmission of ESI discovery providing basic information including the number of electronic media, the unique identifiers of the media, a brief description of the contents, including a table of contents if created, any applicable bates ranges, and any necessary passwords to access the content. The USAO shall retain a write-protected copy of all transmitted ESI as a preserved record to resolve any subsequent disputes.

5. Access to Discovery for In-Custody Defendants: Subject to any limitations imposed by any protective or other order, the USAO, CDA (if one is appointed), and counsel for any defendant in custody will attempt to arrive at reasonable procedures that will enable defendants and their counsel to review discovery produced in the electronic formats specified in (D)(4) above. If the USAO, CDA, and counsel are unable to arrive at such procedures, the issue shall promptly be brought to the court’s attention. Counsel for defendants housed at San Bernardino Central Detention or West Valley Detention Center or at Santa Ana City Jail shall be authorized by this order to take their personal laptop computers into those facilities in order to assist counsel in reviewing discovery with defendants housed at those facilities. No further order authorizing such a use of personal laptops shall be required.
F. APPOINTMENT OF COORDINATING DISCOVERY ATTORNEY

1. At the initial status conference, the court will consider whether to appoint a CDA from the available national CDA and litigation support group, or, upon a proper showing that the national CDA is unavailable and case efficiency requires appointment of a local CDA, a local CDA. Any CJA Defense Counsel, DFPD, or any indigent pro se defendant may make a request for a CDA, and such request should indicate how the appointment of a CDA will benefit the majority of the defendants who have qualified for appointment of counsel or other ancillary services under the Criminal Justice Act (“CJA defendants”). Where multiple defendants are represented by the FPDO and CJA Defense Counsel, the FPDO may opt to receive discovery directly from the USAO, despite the appointment of a CDA.

2. On the appointment of a CDA, the CDA, FPDO, and/or CJA Defense Counsel will confer regarding general and common discovery issues. The scope of the CDA’s duties are defined by this Order, which may be supplemented or revised as necessary.

3. The CDA shall be responsible for accepting discovery from the USAO and duplicating and distributing the discovery to the FPDO, if applicable, the CJA Defense Counsel, and indigent pro se defendants. The CDA will coordinate with the USAO on behalf of the FPDO, the CJA, and indigent pro se defendants regarding any additional discovery issues and needs, including any need to obtain copies of digital data in original format.

4. The CDA shall assist the FPDO, if applicable, the CJA Defense Counsel, and indigent pro se defendants in making discovery materials.
accessible to in-custody CJA and indigent pro se defendants. The CDA will coordinate with each institution housing in-custody FPDO, CJA, and indigent pro se defendants to determine what limitations to discovery access exist for defendants housed in the institution, and will attempt to provide access to discovery within those limitations if possible.

5. The CDA shall provide any additional discovery support service as agreed on by the majority of FPDO, CJA Defense Counsel, and indigent pro se defendants. The CDA also shall identify and oversee any discovery issues that are common to a majority of defendants.

6. It is the obligation of each FPDO, CJA Defense Counsel, and indigent pro se defendant to confer with the CDA directly on issues of discovery. It is the responsibility of the CDA to address discovery issues with the objective of avoiding or reducing potential repetitive costs that would be incurred if FPDO, CJA Defense Counsel, and indigent pro se defendants individually employed ancillary services to handle the discovery in the case.

7. The USAO shall provide one complete set of all discovery materials directly to the CDA and shall not thereafter be responsible for providing any of the discovery materials provided to the CDA to any of the FPDO, CJA Defense Counsel, or indigent pro se defendants, except where the FPDO has opted not to utilize the services of the CDA. The USAO shall be responsible for maintaining the originals of all discovery and evidence in the case and shall make originals available for inspection and copying by the defense on reasonable notice.
8. Nothing in this Case Management Order regarding the appointment or duties of a CDA shall be interpreted to be a restriction on or interference with defense counsel’s obligations to their individual clients. The CDA shall in no way replace or interfere with defense counsel’s efforts on behalf of their clients. The representation of each defendant remains the responsibility of the counsel of record for that defendant or the pro se defendant. Discovery issues specific to any particular defendant, including Brady, Giglio, and related issues, should be addressed by individual defense counsel or the pro se defendant directly with the USAO and not through the CDA.

9. To the extent that any defendant is represented by the FPDO and the FPDO has opted not to utilize the services of the CDA, the USAO shall produce discovery directly to the FPDO according to the provisions in (D) above. The CDA will coordinate with the FPDO (if assigned to a given case) for the benefit of all CJA Defense Counsel and indigent pro se defendants to provide appropriate services and to employ available support and equipment from the FPDO.

G. FUNDING FOR ADDITIONAL ANCILLARY SERVICES

1. For CJA Defense Counsel and indigent pro se defendants, all requests for funding for ancillary services (duplication, experts, investigators, paralegals) shall be made to the CJA Supervising Attorney’s office. All requests for funding for domestic travel shall also be made to the CJA Supervising Attorney’s office. All other funding requests shall be made by ex parte application under seal and in camera to the court.
2. If a CDA has been appointed, before requesting funding for additional discovery-related services, any CJA Defense Counsel or indigent pro se defendant shall confer with the CDA to determine whether the scope of the additional discovery-related services has been or could be addressed by the CDA. Any application for additional discovery-related services shall include a description of the efforts to coordinate with the CDA and why such services cannot be provided by the CDA.

H. DEFENDANT-COUNSEL COMMUNICATIONS

Every CJA Defense Counsel must meet with his or her client regularly. Telephone calls and visits with defendants by a paralegal or investigator are not sufficient compliance with this provision.

I. DEFENSE RESPONSE

1. Defense counsel may respond to this Order or to any response filed by the USAO;

2. Defense counsel may add information on matters not necessarily covered by this Order.

J. SECOND STATUS CONFERENCE: All parties and their counsel shall appear for a second status conference in this matter on [date 35 calendar days after First Status Conference].

K. SECOND STATUS REPORT OF GOVERNMENT: By not later than [date 7 calendar days after First Status Conference], the USAO shall provide, in writing, to defense counsel and pro se defendants, a proposed schedule for all of the items set forth in Sections (J)(2) through (J)(4) below. By no later than [date 14 calendar days after First Status Conference], defense counsel and pro se defendants shall provide, in writing, to the USAO, any objections and/or proposed modifications to the proposed

Complex Case Management Order
schedule. After considering any objections and/or proposed modifications, by no later than [date 21 calendar days after First Status Conference], the USAO shall file a document entitled “Second Status Report,” which shall:

1. Update or correct all information provided in the First Status Report pursuant to Section (B)(1)-(6) above.

2. Provide an updated proposed schedule for production of discovery, including production of discovery by the defense. In the event that production of discovery will not be completed within 14 calendar days of the second status conference, provide a proposed schedule for monthly telephonic status conferences between the USAO and counsel for all defendants to resolve ongoing discovery issues. The USAO shall file a document entitled “[#] Status Report” within 4 business days of each status conference.

3. Propose a trial date. Concurrently with the Second Status Report, the USAO shall file proposed findings and an order regarding excludable time under the Speedy Trial Act with respect to the proposed trial date. At the Second Status Conference, the court shall seek defendants’ concurrence to the proposed findings and order with respect to the trial date selected by the court. Such concurrence shall be without prejudice to additional requests by the USAO or any defendant for continuances of the trial date based on a showing of good cause.

4. Propose schedules for at least the following:
   (a) Completion of discovery production;
   (b) Motions to compel or other discovery motions;¹

¹ FPDO and CJA Defense Counsel shall meet and confer with the USAO, either in person or telephonically, to attempt informal resolution of discovery disputes prior to the filing of any motions. Discovery motions concerning ESI production
(b) Motions regarding joinder and severance;

(b) Motions challenging Title III intercepts;

(c) Motions to suppress any other evidence;

(d) Other pretrial motions dispositive as to all or any portion of the indictment;

(e) Motions in limine;

(f) Completion of plea negotiations, if appropriate;

(g) Provision by the USAO (if 10 or more defendants remain pending trial) of a proposal for dividing the charges in this case into a series of manageable trials, with the objective (if possible) of having every remaining defendant subjected to only one trial, which proposal should contain an explanation of the basis for the proposed division, and should propose the sequence in which the trials should be conducted;

(h) Disclosure by the USAO of Federal Rule of Evidence 404(b) evidence for trial;

(i) Disclosure by the USAO of Federal Rule of Criminal Procedure 12(b)(4)(B) evidence subject to suppression under Rule 12(b)(3)(C), not earlier designated as such pursuant to Rule 16 disclosures;

(j) Disclosure by the USAO and defense of any testifying experts;

(k) Disclosure by the USAO and defense of discoverable witness statements, including grand jury transcripts, not earlier produced;

shall 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.
(l) Disclosure by the USAO of testifying informant information, including Giglio material, not earlier produced as part of the discovery;

(m) Provision by the USAO of prospective witness lists for trial;

(n) Provision by the USAO of prospective exhibit lists for trial.

5. Confirm that the instructions required by Section (D)(3) above have been provided, and list the individuals to whom these instructions have been provided.

6. Confirm that procedures for providing discovery to defendants in custody have been arrived at or identify the issues preventing the implementing of such procedures for consideration by the court.

7. Provide any other information that may assist the court, the USAO, or the defense in handling this matter efficiently and cost-effectively.

L. DEFENSE RESPONSE

1. Defense counsel shall file any response to the Second Status Report not later than [date 28 calendar days after First Status Conference];

2. Defense counsel may add information on matters not necessarily covered by this Order.

M. MANDATORY CHAMBERS COPIES

Paper chambers copies of all documents are mandatory. [Set forth instructions for delivery of chambers copies. For example: The USAO must deliver Chambers copies to the box outside of Chambers by noon on the day after filing. Defense counsel may provide Chambers copies by regular mail. If counsel provide copies by Federal Express, they should not require a signature. The court will not rule on stipulations or ex parte applications until Chambers copies have been received.]

N. E-FILING DOCKETING
The captioned title of every pleading shall contain the name of the first-listed defendant as well as the name(s) and number(s) (in the order listed in the indictment) of the particular defendant(s) to whom the pleading applies, unless the document applies to all defendants. The individual defendant’s registration number (if known) should be provided on any document pertaining to defendant’s custody status (e.g., requests for transfer, medical requests). All parties shall docket items only as to the particular defendant the item pertains to, not as to all defendants, unless the item pertains to all.

With the exception of documents filed under seal or in camera, every pleading shall be electronically filed in such a way that it is clear from the docketing entry to which defendants it applies. The outer envelope containing any pleading filed under seal should identify only the case title with first-listed defendant and case number, and should state that the document is filed under seal.

O. SPECIAL REQUESTS

Requests for any of the following shall comply with the following requirements:

1. **Bail Reviews**: Any request for a bail review based on changed circumstances or information not previously presented to the magistrate judge shall be addressed in the first instance to the magistrate judge and shall be served on both opposing counsel and Pretrial Services.

2. **Pre-Plea Reports**: Any request for a pre-plea report by the Probation Office shall be supported by a showing of good cause, shall propose a schedule for consideration and entry of a guilty plea that comports with any schedule set by the court for completion of plea negotiations and entry of guilty pleas and provides at least six weeks for the Probation Office to prepare the pre-plea report, and shall be served on both opposing counsel and the Probation Office.
3. **Custody Transfer Requests:** Any request by an in-custody defendant for a transfer to a different custodial location shall be made only after consultation with the United States Marshals Service, shall include a statement of the position of the United States Marshals Service regarding the proposed transfer, and shall be served on both the USAO and the United States Marshals Service.

4. **Travel:** Any request by a defendant for a modification of release conditions to permit travel shall be supported by a showing of good cause, shall be made only after consultation with both Pretrial Services and the USAO, shall include a statement of the positions of both Pretrial Services and the USAO, and shall be served on both Pretrial Services and the USAO.

5. **Medical Treatment:** Any request by an in-custody defendant for an order requiring medical treatment shall be made only after consultation with the custodial facility and after the submission to the custodial facility of a written waiver from the defendant permitting the provision to that defendant’s counsel of any medical records relevant to the request, shall include a statement of position of the custodial facility, or a statement regarding defense counsel’s attempt to obtain the facility’s position, and shall be served on both the custodial facility and the USAO.

IT IS SO ORDERED.

DATE: ______________  ___________________________________________

United States District Judge

26
Complex Case Management Order
Viewing Search Results
After a search, dtSearch will display the results of the search. The top half of the dtSearch window will list all of the files retrieved in the search, and the lower half will show the first document in the list, with hits highlighted in yellow.

1. To select a document to view from the search results list, double-click on it.
2. To jump to the next hit in a document window, click Next Hit on the button bar (or press SPACEBAR). Press Ctrl-SPACEBAR, or click the Next Doc button, to go to the next document.
3. To change the way search results are sorted, click on one of the column headers (Name, Score, Location, Date, etc.).
4. Click the Launch button to open a document in the application associated with it. For example, a Word document would be launched in Microsoft Word.

To view or reuse a prior search request, click the Search History tab in the Search dialog box.

Create a Quick Summary of Your Search Results
An easy way to see all hits in all retrieved documents is to build a search report. A search report shows all hits along with the amount of context that you request.
2. Enter the number of words (or paragraphs) of context that you want dtSearch to include in your search report and click OK to generate the report.
3. The search report will open in your word processor so you can edit or print it.

dtSearch Quick Start
To get started with dtSearch, the first step is to build an index of your documents. Once the index is built, dtSearch can use it to search your documents quickly.

Indexing Documents
1. Choose Create Index from the Index menu.
2. In the Create index dialog box, enter a name for the index and click OK.
3. dtSearch will ask if you want to add documents to the index. Click Yes to go to the Update Index dialog box.
4. Click Add folder... to add a folder to the list of folders to index.
5. Click Start Indexing to begin adding documents to your index.
dtSearch automatically recognizes many popular file types. For a complete list of the file formats that dtSearch supports, see the dtSearch website.

Updating an Index
If you edit or add to your documents, you will need to update your index to reflect the changes.
To update your index, choose Update Index in the Index menu (or press Ctrl-U). Check the Index new or modified documents box and the Remove deleted documents box, and then click the Start Indexing button.
To schedule automatic index updates, click Index > Index Manager and click the Schedule Updates button.

International Language Support

Search fuzziness adjusts from 0 to 30 so you can fine-tune fuzziness to the level of OCR or typographical errors in your files. A search for alphabet with a fuzziness of 1 would find alphabet; with a fuzziness of 3, it would find both alphabet and alphabet. Fuzziness is not built into the index, so you can vary fuzziness at the time of each search.

Search fuzziness is based on the spellings of the words. For example, if you search for the word "check", but there is a spelling error and the word is spelled "check", the fuzziness setting would determine if the search result returned the word "check" or not.

Fuzzy searching uses a proprietary algorithm to find search terms even if they are misspelled. dtSearch recommends fuzzy searching for searching emails, OCR text, or any other text that may contain misspellings.

dtSearch includes Unicode-compatible file parsing, to convert input data to Unicode. dtSearch automatically recognizes all Unicode-supported encodings, representing hundreds of international languages.
Searching using the Index

1. Click the Search button on the dtSearch button bar, or press Ctrl-S, to open the Search dialog box.

2. Enter a search under Search Request.

3. Select any items under Search features (such as fuzzy searching) that you want to use.

4. Click Search to begin the search.

Search Types

**Any words:** use quotation marks around phrases, put + (plus) in front of any word or phrase that is required, and - (minus) in front of a word or phrase to exclude it. Examples:

- banana pear "apple pie"
- "apple pie" -salad +"ice cream"

**All words:** like an “any words” search except that all of the words in the search request must be present for a document to be retrieved.

**Boolean search:** a group of words, phrases, or macros linked by connectors such as AND and OR that indicate the relationship between them. Examples:

<table>
<thead>
<tr>
<th>Search Request</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>apple and pear</td>
<td>both words must be present</td>
</tr>
<tr>
<td>apple or pear</td>
<td>either word can be present</td>
</tr>
<tr>
<td>apple w/5 pear</td>
<td>apple must occur within 5 words of pear</td>
</tr>
<tr>
<td>apple not w/5 pear</td>
<td>apple must occur, but not within 5 words of pear</td>
</tr>
<tr>
<td>apple and not pear</td>
<td>only apple must be present</td>
</tr>
<tr>
<td>name contains smith</td>
<td>the field name must contain smith</td>
</tr>
</tbody>
</table>

Booleans can be combined in any way. For example, apple and pear or orange juice could mean (apple and pear) or orange, or it could mean apple and (pear or orange).

You can use variable term weighting in a search request to weigh some words more heavily than others in ranking search results. Example: apple:5 and pear:3

Search Features

**Stemming** searches other grammatical forms of the words in your search request. For example, with stemming enabled a search for applies would also find apply, applying or applied.

**Phonic search** finds words that sound similar to words in your request, like Smith and Smythe.

**Fuzzy search** sifts through scanning and typographical errors. Fuzziness adjusts from 1 to 10 depending on the degree of misspellings. A search for alphabet with a fuzziness of 1 would find alphaqet; with a fuzziness of 4, it would find both alphaqet and alpkaqet.

**Synonym searching** tells dtSearch to use a thesaurus to automatically expand a search to include synonyms or related concepts, including three optional levels. (Click Browse thesaurus to browse the entire thesaurus.)

To see how stemming, phonic searching, fuzzy searching or wildcards will affect your search, click the Browse Words button.

To browse the thesaurus used for synonym searching, click the Browse Thesaurus button.

Click the Fields button for a list of searchable fields, if you want to limit your search to a particular field.

More Search Options

To search without an index, or to search by filename, date, or size, click the More search options tab.
Best Deals for Adobe Acrobat Pro

There are several options for purchasing Adobe Acrobat Pro DC directly from Adobe.

The cost for a single perpetual license for DC Pro (the latest version) is $449. A perpetual license is a one-time purchase that allows one user to install the program on two different computers. Once you have purchased the license, you have the option of upgrading it to the newer version for $199.00 whenever a newer version is released. To be eligible to upgrade to the newest version, you have to have a license that is either version X or XI (versions 9 and older are not eligible).

Alternatively, you can purchase a single subscription based license on a monthly basis for $14.99 per month (with a one year commitment). All updates are included with this price, and like the first option, you can install the license on two computers.

You can compare the plans or purchase Adobe Acrobat here: acrobat.adobe.com/us/en/pricing/pricing.html

A good explanation of Perpetual vs. Subscription can be found here: blogs.adobe.com/acrolaw/2015/05/a-new-way-to-buy-acrobat-dc-subscription/

One way that many panel attorneys have been able to obtain Adobe Acrobat Pro at a discount is through their Educational Program. If the purchaser is in any way affiliated with an educational institution (i.e. student, faculty, volunteer, or knows somebody who is and can ask them to purchase the program for you), the cost for the program drops to $119 and can be purchased at student bookstores or their online equivalents. Again, this is for a single license that can be installed on two computers.

Though they take more leg work, there are sources outside of Adobe for purchasing Acrobat which may be less expensive (for example, some have found web sites that offer the single license package for as little as $149). Adobe Acrobat XI Pro, which is very similar to Acrobat DC Pro in terms of functionality, may also be available on these sites for a reduced price. Availability and duration of sales vary. Some web sites that are worth looking into are:

- amazon.com
- CDW.com
- www.topsoftdeals.com
- technetmicro.com
- nextag.com (here you can compare prices from a range of retailers)
Caution: when scanned paper is turned into PDF format, it can be made searchable through a process called “OCR” (Optical Character Recognition). OCR will try and translate an image to text, but it can be inaccurate, especially when dealing with poorer quality images. When searching PDF files you might not get a complete set of results.

Find
- Go to the Edit menu and select Find or press Ctrl+F.
- Your cursor will move to the Find box on the toolbar.
- Enter text – each time you press the enter key, it will go to that text in the PDF file.

Advanced Search
- Go to the Edit menu and select Advanced Search or press Shift+Ctrl+F.
- A search window will appear enabling you to look for search terms in multiple PDFs. For example, you can search across all PDFs in a specific location or all files.
- With Standard or Pro, you can save your search results to a PDF or CSV (spreadsheet) file.

*Recognize Text (a.k.a. OCR or Optical Character Recognition)
- If a PDF is not searchable you can make it so by running the “Recognize Text” process.
- From the “Tools” pane select “Recognize Text”. You can run the process on a single file, or multiple files.

*Bookmarks
- A “bookmark” is a link with text in the “Bookmarks” panel. Each bookmark goes to a different view or page in the document, and allows one to jump to a destination in the PDF, to another document, or to a webpage. They can function as a table of contents.
- Bookmarks can also be used to create document breaks within a PDF. This is also called unitizing, and by bookmarking a PDF you can allow people to review pages on a document level in addition to a page level. We suggest that a bookmark with the bates number as the name of the bookmark be used to label each new document within the PDF file.

*Comments (a.k.a. Annotations or Sticky Notes)
- Comments are notes and drawings that communicate ideas or provide feedback for the PDF files. You can type a text message using the Sticky Note tool, or you can use a drawing tool to add a line, circle, or other shape and then type a message in the associated pop-up note.
- Most comments include two parts: the icon, or markup, that appears on the page, and the text message that appears in a pop-up note when you click or double-click the icon or place the pointer over the icon.

* Not available in the free Acrobat Reader
Acrobat Pro Document Unitization

The following technique can be used to split up a PDF file with many pages into smaller files:

1. **Create bookmarks:**
   a. Add a bookmark to the very first page of the document. Continue to add bookmarks to pages where splits should occur (the beginning pages of a sub-documents within the larger file).
   b. The bookmark names will become the new file names.
   c. Give a unique name to each bookmark (so that the new file names will also be unique).
      i. If the pages are bates numbered, consider using the bates number as a prefix for the bookmark name.
      ii. Try not to use extraneous punctuation marks in the bookmark names as this may cause a conflict during the splitting process. Using dash characters "-" and underscore characters "_" are okay, but avoid using characters like “?!\&'%^”.

2. **Set up the split:**
   a. Acrobat DC Pro: From the “Tools” tab or side menu...choose “Organize Pages”, then select “Split”.
   b. Acrobat 11 or lower: Select “Split” from the “Pages” group in “Tools”.
   c. Choose to Split by “Top Level Bookmarks”, the click on the “Output Options” button.
   d. Choose “Use bookmark names for file names” and click “OK”.

3. **Run the split:**
   a. Acrobat DC: click the lower “Split” button (next to “Output Options”).
   b. Acrobat 11 or lower: Click the “OK” button within the “Split Document” dialog.

**Acrobat DC:**

**Acrobat 11 or lower:**
We are pleased to announce that the Defender Services program has contracted with Casepoint, LLC to provide an online document review platform for CJA panel attorneys and federal defender offices (FDOs) in select federal Criminal Justice Act (CJA) cases. Casepoint LLC hosts Casepoint, an online, e-Discovery platform used by law firms, major corporations and governmental legal departments. Casepoint includes computerized early case assessment, technology assisted review (TAR), cloud analytics, data processing and a fully hosted review platform. The platform has an easy-to-use interface which makes its accessible to all end users, from novice users to legal professionals who are experienced with other document review platforms.

Casepoint is designed to assist attorneys and their staff in organizing, managing and analyzing large volumes of discovery. If approved, a set amount of case material from CJA / FDO cases can be hosted on Casepoint without the need to seek funding from the trial court. If a case has more discovery than can be hosted under the contract, a discounted rate is available for larger cases needing to host additional data. Using a secure, web-hosted document review platform such as Casepoint is advantageous in multi-defendant cases with large volumes of information. Case materials are located in one central repository and easily reviewed, tagged and accessed by all defense teams from wherever they are as long as they have an internet connection. This greatly alleviates the need for panel attorneys to have specific hardware, software or IT support usually necessary to utilize similar review platforms on your local office network. Along with the online document review platform, Casepoint, LLC provides project management expertise and training for all users of the system.

Casepoint and other legal review platforms are different from online storage services such as Box.com and Dropbox. Storage services such as Box.com and Dropbox are built for the cloud
storage and sharing of files with limited other functionality whereas Casepoint is a document review tool developed specifically for legal work. Some key features of Casepoint that will be key to the management of discovery include the ability to maintain private notes in a multi-defendant case that cannot be seen by other legal teams on the case, universal bulk tagging, filtering, and annotation which can be shared by all legal teams; review of e-discovery without changing any of the underlying background information; and having the option to view many file types within the platform without having the original program in which the document was created in on your computer (e.g. you can see an Excel spreadsheet without having Microsoft Excel installed on your computer). NOTE: If you have a CJA case that could benefit from the short-term storage of data or the transfer of data on the cloud, please contact the National Litigation Support Team (NLST) as we have a national contract with Box.com and can provide hosted space at no cost to panel attorneys.

To assess whether your case qualifies for Defender Services funded secure hosted space, please do the following:

1. Have an attorney on the case contact Kelly Scribner at 510-637-1952 to discuss the discovery you wish to have hosted. Make sure to identify whether the local federal defender office is involved as well and whether there are any retained counsel. To assist you prior to your call, please review the Initial Discovery and 3rd Party Data Assessment Checklist on fd.org at https://www.fd.org/sites/default/files/Litigation%20Support/initial-discovery-assessment-checklist.pdf as we will review the answers to these questions in determining whether the use of Casepoint is appropriate for your case.

2. Schedule a demonstration of Casepoint for all parties with the NLST to ensure that the platform technically fits your needs and that the all defense teams are comfortable with the user interface.

3. Discuss the option of using Casepoint with all defense teams and identify any parties who do not wish to participate and have access to the platform.

Allocation of hosted space will be based on a first come first serve basis and only for cases in which there is a benefit to having discovery hosted. Space is limited and this is a service for all CJA panel and FDO attorneys, so we cannot guarantee there will be space available for every case. If space is not available, Casepoint will provide a reduced rate for CJA panel attorneys and FDOs.

Please do not hesitate to contact either Kelly Scribner (kelly_scribner@fd.org) or Sean Broderick (sean_broderick@fd.org) at 510-637-3500 if you have any questions.
To assist CJA panel attorneys who need to share and transfer e-discovery in their multi-defendant CJA cases, the National Litigation Support Team (NLST) has obtained web-hosted repository ("cloud") space from Box.com. There is no cost to panel attorneys for using this service.

Box.com is a simple cloud-based collaboration program that allows users to store, access, share, and transfer electronic files and documents. The service encrypts all data and has additional security features. Users can store an unlimited number of files, for their own use or to share with others, without having to use remote access to office computers. Defense teams can use different devices (such as computers, tablets, or smartphones) to access case data anywhere they can connect to the internet. This allows CJA panel attorneys to share discovery and work product easily and efficiently in a secure environment.

Box.com is being used by the Department of Justice (DOJ) as their cloud service to distribute e-discovery to the defense. DOJ evaluated it against other similar products and concluded it best met their security standards.

Box.com is committed to ensuring that your data will remain as secure as possible, and providing strong customer support. They have worked closely with the NLST in designing a cloud service that effectively addresses CJA counsels’ growing problem of moving and sharing large volumes of data. The NLST will work directly with each defense team to set up their cloud case folders, and to provide ongoing support of their use of Box.com.

The NLST will manage:

1. creating case folders to hold electronic information on a case in the cloud,
2. inviting team members ("collaborators") to help them get access to the cloud data, and,
3. granting rights of different team members to get into specific folders.
Because cloud contracts like this store case information on servers owned by Box.com, attorneys remain ultimately responsible for the use of this service. Before using it, CJA members should review their local bar opinions regarding the use of cloud computing and storage.¹

Once approved, the NLST will send you a form asking for the case details including who will serve as the “point of contact” for each defense team, and who on the team should be given access to the what files that have been stored on the cloud. Note that additional team members can be added later. The NLST will set up a short session to show all those who will use this cloud service how to navigate the system, and how to upload and download data. The NLST will be the team’s first point of contact if there are any questions about using Box.com, technical questions, or any concerns regarding using this cloud-based case information repository.

Please note that Box.com does not offer advanced e-discovery features found in online document review programs such as Relativity, Summation, or Catalyst. It does not have a database and other advanced tools for organizing, reviewing, and analyzing e-discovery. Rather, its purpose is for short-term storage and transfer of information in the “cloud.”

When the case has concluded, (or sooner if counsel no longer needs this service), the CJA lawyer must delete all case materials from Box.com. The NLST will help ensure the case files are deleted, and the case is properly closed. Counsel should always maintain a copy of all files on their office computer system (besides the information stored in the cloud), as only duplicate files should be stored on Box.com.

If you are interested in using Box.com for a multi-defendant case, or have further questions, please contact:

Kalei Achiu (kalei_achiu@fd.org or 510-250-6310) or,
Alex Roberts (alex_roberts@fd.org or 510-637-1955) or,
Kelly Scribner (kelly_scribner@fd.org or 510-637-1952.

¹ At least 19 state bar associations have written ethics opinions on its member’s responsibilities while using cloud computing services. Each of the 19 opinions permit using cloud computing but hold attorneys to a duty of “reasonable care,” with the specific requirements of reasonable care varying with each state. https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html
We are pleased to announce the continued availability of a dtSearch Desktop software license to CJA panel attorneys with current, active cases.

dtSearch is a popular search and retrieval program, and it is the search engine utilized in well known computer programs such as Forensic Tool Kit (FTK, a computer forensic tool), CaseMap and Adobe Acrobat Pro. This type of program is a useful tool to assist legal teams in searching discovery, creating brief banks, and viewing different file types (including non-PDF files) even if you don’t have the associated application. We have a limited number of licenses available for CJA panel attorneys to use for free (a $200 value).

The program provides great functionality in searching both electronic documents and paper documents that are subsequently scanned and converted to a text searchable format, especially since it can search and retrieve information in many different file types. dtSearch is a user friendly software program which provides immediate results and utility for even the novice computer user. As electronic discovery in federal criminal matters continues to grow in volume and in the variety of formats, dtSearch is a useful tool for CJA panel attorneys faced with the daunting task of organizing and searching through their case material.

To obtain the software, please fill out the dtSearch Request Form located at:

https://docs.google.com/forms/d/1KibRVAtcZdzCzj8HeGVWkAnZK3YN_aD6NWOaoW_cCdE/viewform

When finished filling out this form, press the "submit" button on the bottom of the form. This will attach your completed form to an email message sent to Assistant National Litigation Support Administrator Kelly Scribner (kelly_scribner@fd.org). You will then receive an email with download instructions and the activation code necessary to obtain your free copy of the dtSearch Desktop. Please allow up to 5 business days to process your request. Each user license can be installed for that user on two machines.

You must have an active appointed case to continue to utilize the license. If you are no longer on the panel and don't have an active appointed case, we request you return the license to the National Litigation Support Team (NLST) by contacting Kelly Scribner so the license can be used by other CJA panel attorneys. Like most litigation software programs, this program was developed for Windows-based operating systems and does not work with Macintosh operating systems.

For technical support or if you have any questions regarding the utilization of dtSearch within your office, please contact either Alex Roberts or Kelly Scribner (members of the NLST) at 510-637-3500, or by email: alex_roberts@fd.org, kelly_scribner@fd.org. If you want to learn more about dtSearch, go to http://dtsearch.com/.
Web Resources

- Litigation Support page of FD.org
  (fd.org/odstb_LitigationSupport.htm)

- National Litigation Support Blog
  (NLSBlog.org)

- Guidelines for Administering CJA and Related Statutes
  (uscourts.gov/defenderservices/volume7.cfm)
The Criminal ESI Protocol

ESI PROTOCOL: JETWG RECOMMENDATIONS FOR ESI

WHAT IS LITIGATION SUPPORT

The Department of Justice/Administrative Office Joint Working Group on Electronic Technology (JETWG) has developed a recommended ESI protocol for use in federal criminal cases. Entitled "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases", it is the product of a collaborative effort between the two institutions and it has the DOJ leadership's full support.

The primary purpose of the ESI protocol is to facilitate more predictable, cost-effective, and efficient management of electronic discovery and a reduction in the number of disputes relating to ESI. The protocol provides a mechanism, through a meet and confer process, to address problems a receiving party might have with an ESI production early in a case, and to discuss the form of the discovery that the party receives. The participants on both sides of JETWG are intimately familiar with the day-to-day challenges attorneys face in criminal cases, and the protocol reflects a pragmatic approach to the problems both prosecutors and defense attorneys face when dealing with electronic discovery.

JETWG negotiated and drafted the protocols over an 18-month period. The joint working group has representatives from the Federal Defender Offices, CJA Panel, Office of Defender Services, and DOJ, with liaisons from the United States Judiciary, Andrew Goldsmith, the DOJ National Criminal Discovery Coordinator, and Sean Broderick, the National Litigation Support Administrator, serve as co-chairs. Donna Ellen, Federal Public Defender for the Middle District of Florida, Doug Mitchell, CJA Panel Attorney District Representative for the District of Nevada, Bob Burke, Chief of the Training Branch for Office of Defender Services, and Judy Mroczka, Chief of the Legal and Policy Branch for Office of Defender Services, round
Selected Lit. Support Tools

Free
- Acrobat Reader
  search PDF files
- IRFanView
  universal image reader
- VLC Media Player
  universal media player
- FTK Imager
  reads forensic image files

Low-Cost
- Adobe Acrobat Pro
  make PDF files searchable
- CaseMap
  case organization and search
- TrialDirector
  trial presentation
- dtSearch
  Advanced search and retrieval
CJA Technology Resources

CJA Panel Attorney Software Discounts

https://www.fd.org/litigation-support/cja-panel-attorney-software-discounts

<table>
<thead>
<tr>
<th>Software</th>
<th>Discount/Price</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CaseMap/DocManager/TimeMap Bundle</td>
<td>$580</td>
<td><a href="mailto:PMsales@lexisnexis.com">PMsales@lexisnexis.com</a></td>
</tr>
<tr>
<td></td>
<td>No annual maintenance or subscription fees</td>
<td></td>
</tr>
<tr>
<td>TrialDirector</td>
<td>50% discount $397.50 + $159 maintenance fee</td>
<td>800-828-8292</td>
</tr>
<tr>
<td>dtSearch Desktop</td>
<td>Free (normally $200)</td>
<td><a href="http://nlsblog.org/2014/03/25/dtsearch-desktop/">http://nlsblog.org/2014/03/25/dtsearch-desktop/</a></td>
</tr>
</tbody>
</table>

Alex Roberts  alex_roberts@fd.org
Kelly Scribner  Kelly_scribner@fd.org
510-637-3500

National Litigation Support Blog for Federal Defenders and CJA Practitioners

https://nlsblog.org/

Defender Services Litigation Support

https://www.fd.org/litigation-support/who-national-litigation-support-team

CJA Funding of Technology

The rules governing the use of CJA funds for hardware and software are set out in the Guidelines for the Administration of the Criminal Justice Act, Vol. VII to the Judiciary Policies and Procedures. They can be found at http://www.uscourts.gov/sites/default/files/vol_07.pdf. Additional information is available at the Litigation Support tab of https://www.fd.org/.

1. What can be purchased with CJA funds?
a. Services of experts, such as “computer systems and automation litigation support personnel.” §320.70.10
b. Computer hardware. §320.70.40
c. Computer software. §320.70.40
d. Unusual or extraordinary expenses can be considered “other services necessary for an adequate defense.” §320.70.30

**NOTE:** CJA attorneys are expected to use their own office resources, including secretarial help, for work on CJA cases. In the context of technology, CJA funds can be authorized if the item is “not typically available in a law office.”

2. When do you need prior authorization to purchase equipment?

<table>
<thead>
<tr>
<th>Under $50</th>
<th>No authorization needed.</th>
<th>No receipt needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>$50-$800</td>
<td>No authorization needed.</td>
<td>Receipt must be uploaded to voucher.</td>
</tr>
<tr>
<td>$800-$2,400</td>
<td>Must notify the Litigation Support Team to discuss the purchase and receive guidance and a recommendation.</td>
<td>Receipt must be uploaded to voucher.</td>
</tr>
<tr>
<td>More than $2,400</td>
<td>Must notify the Litigation Support Team to discuss the purchase and receive recommendation.</td>
<td>Receipt must be uploaded to voucher.</td>
</tr>
<tr>
<td>More than $10,000 for combined purchases.</td>
<td>Prior to requesting authorization from District Court and Circuit Court, must consult with National Litigation Support Team in Defender Services Office. 510-637-3500</td>
<td></td>
</tr>
</tbody>
</table>
3. How do you obtain authorization for hardware/software?

A. If you meet the $800 threshold, contact the Litigation Support Team and receive their recommendation.
B. Submit an Auth, through eVoucher. Include the following information in the form of a memorandum or letter, uploaded to the documents page:
   1. The name of the product (or description of services) that you want to have funded.
   2. What the thing you want to buy will do.
   3. Why this is necessary to present your client’s defense.
   4. Whether any co-defendants will benefit from the purchase of this equipment.
   5. How much it costs.
   6. Why this is not something (or someone) that is typically available in a law office.
   7. Whether you will need a person to help you use the purchase.
   8. How much that person’s services will likely cost. (hourly rate x estimated hours)
   9. A statement verifying that you have complied with the rule requiring contacting the Litigation Support Team.
   10. Your commitment and agreement to turn any product over to either ODS or FDO at the end of your case.
C. Wait to received the approved Auth back from the District Court and Court of Appeals.

4. How do you pay for the hardware/software/services?

A. After you have received authorization, you may pay directly for the equipment and then claim it as an expense on your next CJA20.

   --or--

B. Contact CJA administration and we can arrange to pay directly for equipment, by setting up the vendor in eVoucher.

C. If services are being provided, provide the information to CJA administration and the service provider will be set up in eVoucher. Counsel will then be able to submit the invoices on behalf of the service provider, by using a CJA21.