

ESI Protocol Potential Topics

(Oct. 2019)

ESI Protocol Brainstorming Group Members:

Brian D. Clark (Group Leader)

Claudia T. Morgan (Group Leader)

Tara S. Emory

Laura Farley

Eric Fierro

Claire Hass

Sean Hert

Dawson Horn III

Laura Hunt

Robert D. Keeling III

Jeannine Kenney

Vikram Masson

Hon. Thomas B. Smith

Lea Malani Bays (Steering Committee Liaison)

Andrea L. D'Ambra (Steering Committee Liaison)

Gareth T. Evans (Steering Committee Liaison)

Copyright 2019, The Sedona Conference. All Rights Reserved.



ESI Protocol Potential Topics

1. Bates numbering requirements
 - i. Form of Bates (e.g. whether spaces or special characters are allowed), number of digits, zero padding
 - ii. Unique Bates prefix for each producing party even if related entities
2. Cooperation
 - i. Meet and confer before motions
 - ii. ESI liaisons for parties
 - iii. Agreement on how court assistance will be sought, with court approval
 1. Many ESI orders have built in mechanisms to guide the parties when an agreement cannot be made. This often occurs with search term/search methodology, custodian selection, and working through claims of overbroad and burdensome search results.
3. Date Filtering
 - i. The parties should clarify if this is part of the ESI protocol or as part of the search terms.
4. De-duplication, near duplication, and email thread identification
 - i. Whether thread suppression will be permitted
 - ii. Whether exact deduplication (horizontal) is permissive or required and technical specifications for exact deduplication.
 - iii. Whether deduplication of near duplicates is permitted.
 - iv. Technical specifications for deduplication (including treatment of emails with BCCs in the header).
 - v. What additional metadata fields will be required for global deduplication (e.g. OtherCustodian)
5. Document Sources
 - i. Disclosures:
 - ii. Custodians
 - iii. Noncustodial sources

6. File-type filtering
 - i. Exception files
 - ii. Whether password protected/encrypted files must be produced and disclosed or may be withheld and the effort that a producing party must undertake to identify the password or key.
 - iii. Whether the parties may de-NIST and whether there are other file types not included in the NIST list that may be excluded
 - iv. Whether some notice should be given when files cannot be accessed or searched but are within scope of the search process.
7. Form of production for unstructured data:
 - i. Native vs. static image
 - ii. Native production provisions
 1. How will the parties address files created with software that is either not common (e.g. not created with office productivity software) or proprietary?
 - iii. Static image production provisions
 1. Image specifications
 - a. Will the images be black & white or color?
 - b. What technical specifications will apply to the images (e.g. 300 DPI black and white Group IV TIFF)?
 - c. If black & white images, under what circumstances will the parties provide color images?
 2. Load File specifications (.dat and .opt)
 - a. Will specifications be negotiated in detail or left up to the producing party as long as the agreement that a load file will be included?
 3. Metadata fields
 - a. What metadata fields will be provided by the parties? The agreed-upon listing may differ based on document type (e.g. ESI vs. hard copy).

4. Text files

- a. In what format will text files be provided (e.g. one text file per document)?
- b. What agreement, if any, will the parties reach regarding text for redacted documents and documents which do not contain text (e.g. scanned hard copy documents)?

8. Handling of compressed files

- i. Whether a container file (e.g. zip file) should be treated as a record, and any family relationships between the container document and what is contained in the container?
- ii. Whether context can be gained by maintaining the family relationship of a decompressed file and is lost by failing to maintain family relationships.
- iii. How to address containers within containers?

9. Metadata fields

- i. The relevance of each listed field will be a point of discussion for the parties to a case. Commonly encountered metadata fields are:
 1. Bates fields (begbates, endbates, attachbates, attach range)
 2. Family relationships
 3. Custodian
 4. Record Type
 5. Source Party
 6. Confidential / AEO designations
 7. Original file name of document and subject lines for emails
 8. Author
 9. Relevant date/time for creation and modification (i.e., time zone)
 10. Attachments and number of files attached
 11. Page count
 12. File Size
 13. Directory information: Folder and filepath
 14. Doc Extension
 15. Hashvalue

16. Date/Time Created (for docs)
 17. Date/Time Received (for email)
 18. Date/Time Sent (for email)
 19. Date/Time last modified/accessed
 20. From/To/CC/BCC
 21. ConversationThread
 22. Full Text File Path
 23. OCR
 24. NativeLink
 25. Field required if documents are to be globally deduplicated (e.g., Other/All Custodian, OtherCustodianDirectory)
 26. Field indicating paper documents scanned for litigation and documents containing redactions.
10. Non-Discoverable ESI
 - i. E.g. slack/fragmented data
 - ii. ESI deleted in normal course of business prior to litigation hold
 - iii. Process for approaching seemingly irrelevant data types that become highly relevant further on in discovery
 11. Paper Documents
 - i. Handling of paper documents
 - ii. Unitization
 12. Preservation
 - i. Whether the parties wish to agree on categories of data or information that need not be preserved
 1. And categories of data that shall be preserved?
 - ii. Whether the parties wish to agree on a time period for preservation and production
 - iii. Legal hold
 - iv. Preservation of metadata
 1. impact on collection methods
 - v. exclusion of inaccessible or burdensome data sources (i.e. disaster recovery systems)

13. Privilege Logs/Logging
 - i. Fields to be included in a privilege log
 - ii. Whether categorical privilege logs are permissible, and if so, specifications
 - iii. Discussion of metadata only logs (including the fields to be provided by producing party and concerns regarding whether fields are understandable and legible)
 - iv. Keys that identify individuals in the log, i.e. providing a list of attorneys (in-house and outside counsel)
 - v. Process for challenging privilege
 - vi. Deadline for service of a privilege log
 - vii. How to deal with threads (as opposed to an email chain) on a privilege log (email by email or log inclusive email).
 - viii. Exclusion of categories of documents from logging requirement (i.e. all communications with outside counsel post-complaint regarding the litigating of the matter need not be logged)
14. Processes for addressing redacted content and withheld family members (e.g., how text files will be redacted)
15. Production Media and Contents of Cover Letters
 - i. What production media can be used
 - ii. What information transmittal letters must contain.
 - iii. Procedures for encryption and transmittal of passwords.
 - iv. Place for delivery.
16. Proportionality
 - i. Undue burden/accessibility
 - ii. Categories deemed not reasonably accessible
 - iii. Tiered discovery (See Sedona Principles)
17. Rule 502(b)/502(d) provisions and their state law equivalents
 - i. Clawback procedures
 1. Should 502(b) standard be included in 502(d) for safe measure?

2. What timing is necessary/fair for the producing and receiving party?
 - ii. Limitations on clawback with respect to depositions
 - iii. Notification of privileged material received
18. Search and Production of Document Families
 - i. Whether searches will be run across entire families
 - ii. Production of families where fewer than all documents are responsive, e.g. use of slip-sheets to denote non-responsive, technical issue, or privileged documents.
 - iii. Handling of embedded files – whether embedded files should be processed as family members of an embedded parent document (e.g. extracted as children of the parent) as well as remaining in the parent.
19. Search Methodology, processes, and parameters
 - i. Whether and what document requests can be satisfied in whole or part without need of electronic search methodologies.
 - ii. Whether metadata filtering will be used and how, and what disclosures are required.
 - iii. Processes for agreeing on custodians and related disclosures necessary for meaningful meet and confers.
 - iv. Processes for agreeing on custodial and non-custodial data sources that will be searched, and related disclosures necessary to ensure meaningful meet and confers.
 - v. Processes for agreeing on electronic search methodology and related disclosures.
 - vi. Keywords
 1. Agreements and understandings regarding how terms will be identified.
 2. Processes for negotiations and iterations.
 3. What disclosures will be made to aid the negotiations (hit counts, responsiveness sampling/testing).

4. How disputes will be handled.
5. How the parties will deal with subsequent searches.

vii. TAR

1. Disclosures, agreements, and understanding about whether and what pre-culling prior to TAR ingestion may be used.
2. Disclosures, agreements, and understandings regarding the TAR tool to be used, the workflow/processes to be employed, how and by whom the tool will be trained.
3. Agreements and understandings about what data sources and types might be excluded from the TAR review and how those data sources and types will be reviewed.
4. Agreements and understanding regarding how uncategorized documents will be reviewed.

viii. Requirements for sampling, validation, quality control, and disclosure of related metrics regardless of search methodology.

ix. Identification of specific requests that may require specific or alternative search methodology or parameters.

x. Are there any limitations on the search capabilities of the responding party?

xi. Questions for consideration:

1. How can the responding party maintain control over the identification and collection process as recommended by Sedona Principle 6 while still maintaining cooperative and transparent communications with the requesting party and avoiding bringing disputes to the court?
2. When do disclosures about search terms or other collection methodologies veer into attorney work product protected information?
3. Are there different sets of search terms for collection and to cull pre-review?

4. What information should be part of the negotiation between the parties regarding search (i.e. through email correspondence) versus what information should actually appear in the ESI protocol itself?

20. Security of data

- i. Parties may provide full transparency or represent certain specific security requirements are being met.
- ii. Where highly sensitive data is involved, a party may have a greater need to understand the environment where its produced data will be kept, who will have access, and safeguards to prevent unauthorized access.

21. Structured Data

- i. Process for negotiating what fields to be included and whether disclosures (including of fields, field definitions, database structures) will be made to facilitate negotiations (e.g. sample reports, data dictionaries, etc.)
- ii. Provisions for production of structured data (e.g. report, export, reasonably usable form, other options)
- iii. Methods for producing structured data
- iv. Agree to agree

22. Third parties

- i. What is said in the ESI protocol about applicability to third parties?
- ii. The protocol may state that it is to be applied in whole or in part to third parties.
- iii. Advised to place a proportionality limit on such requirements and require third parties to disclose if the limit applies and what they will do instead before producing; otherwise, third parties sometimes disregard a burdensome protocol in productions.

23. Use of Produced documents