HOGAN & HARTSON

September 2006

WHAT YOU DON'T KNOW CAN HURT YOU: GOVERNMENT E-DISCOVERY IN CRIMINAL INVESTIGATIONS

By Peter Spivack1/

I. INTRODUCTION

Unlike the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure have not yet been revised to address the demands of electronic discovery in criminal investigations. Moreover, the government has learned that the most compelling evidence can often be found in e-mails that reside on backup tapes or deleted documents that have not yet been overwritten. As a result, the government frequently insists on full electronic production, and companies can, and often do, spend millions of dollars complying with government subpoenas. While it remains to be seen whether the amendments to the Federal Rules of Civil Procedure will have an influence on federal judges' willingness to curb the scope of government requests for electronic evidence, the current standard is that arguments of burdensomeness and overbreadth are unlikely to be successful. 2/

This article discusses policies and procedures that counsel might advise a company to take so that a prudent and swift response awaits any unanticipated government inquiries that involve electronic records. The discussion that follows and the attached documents are intended to be useful to any company faced with either the prospect or reality of climbing the mountain of electronic discovery. The attached documents are designed to be only general guidelines, of course.

II. GRAND JURY AND ADMINISTRATIVE SUBPOENAS

Your client's management may be familiar with a seemingly less intrusive means of gathering information during a criminal investigation, namely, grand jury subpoenas or administrative subpoenas.3/ While the issuance of a subpoena may on the surface appear less

---

1/ Peter Spivack is a partner in Hogan & Hartson's White Collar and Investigations Group and a former federal prosecutor. He represents companies and individuals in criminal and civil fraud investigations by state and federal law enforcement authorities.

2/ "Once it is shown that a subpoena might aid the grand jury in its investigation, it is generally recognized that the subpoena should issue." *In re Antitrust Grand Jury Investigation*, 714 F.2d 347, 350 (4th Cir.1983). The party seeking to quash a subpoena must usually show that the requested information bears "no conceivable relevance to any legitimate objective of investigation by the federal grand jury." *In re Liberatore*, 574 F.2d 78, 83 (2d Cir.1978); *In Re Grand Jury Subpoena (Battle)*, 748 F.2d 327, 330 (6th Cir.1984).

3/ Administrative agencies may have very broad subpoena power. For example, under the Inspector General Act, an agency's Office of Inspector General is authorized to issue subpoenas for the production of all information, documents, and documentary evidence necessary to combat fraud and abuse in agency programs and operations. *See* 5 U.S.C. App. 3 § 6(a)(4). The general standards for determining whether an administrative subpoena is enforceable are well-established. A United States District Court will enforce a subpoena if: (1) the subpoena is within the agency's statutory authority; (2) the information sought is reasonably relevant to the investigation; and (3) the demand is not unreasonably broad or burdensome. *See, e.g., United States v. Morton Salt Co.*, 338 U.S. 632 (1950).

intrusive to the day-to-day operations of a company, depending on the actual terms of the request outlined in the subpoena, it may actually be far more invasive as to a company's intellectual capital than a one-time government search. Unlike a search warrant, no probable cause requirement exists for the issuance of a grand jury (or an administrative) subpoena. Therefore, such requests are presumed to be reasonable, but they are often extremely broad. In theory, a subpoena can be quashed if compliance would be unreasonable or oppressive, but such efforts to quash succeed infrequently in the criminal context.

Grand jury subpoenas are issued either to collect documents (a *subpoena duces tecum*) or to compel testimony of company employees (a *subpoena ad testificundum).* Such a document production or testimony request provides the company with the opportunity to prepare its responses or witnesses in advance, and to protect documents that are privileged and confidential from discovery. The grand jury process provides plenty of notice that an investigation is about to commence and, therefore, sufficient time usually exists for consultation with in-house counsel and outside criminal counsel.

A. Subpoena to Produce Documents

In-house counsel may be used to receiving civil discovery requests as a routine aspect of their representation of the company. However, upon receipt of a grand jury subpoena, the company's response to the government should be immediately distinguishable from the often non-cooperative posture adopted by companies engaged in civil litigation. Failing to promptly and forthrightly address a subpoena risks at a minimum the issuance of a search warrant and at the extreme may provide the basis for obstruction of justice charges against the company.

The first step that must be undertaken upon receipt of a subpoena (if it has not been done already) is to send out immediately a communication to all employees who may have documents covered by the terms of the subpoena. 4/ Most public corporations have developed procedures for "litigation holds" that can be used pending further refinement once the defense counsel is engaged. The employees should be informed that such documents, whether in electronic or hard-copy form, must be retained indefinitely, regardless of other corporate document retention policies that may be in existence. The memo should expressly indicate that the duty to preserve relevant documents applies to documents in the office or out of the office in any storage media (home computer, laptop, etc.), as well as documents that may be stored on portable media (flash drives, CDs, floppy disks) or PDAs/BlackBerry devices. Such a communication should spell out explicitly that no document should be destroyed, shredded, removed, or altered in any manner until counsel for the company authorizes the resumption of standard retention practices, and that any violation of this directive will be incur disciplinary action, up to and including termination. To protect the company from the actions of an errant employee, the suspension order should be sent out with a return acknowledgement required from every employee in either hard-copy or electronic form. An example is enclosed at Attachment 1.

4/ The government also take the position that the company is under an obligation to take affirmative steps to preserve documents even prior to the issuance of a grand jury subpoena or other official government request for documents. Under the Sarbanes-Oxley Act, a company may not destroy or alter documents with the intent of impeding or influencing an investigation or *any other matter* within the jurisdiction of a federal agency or department. *See* 18 U.S.C. §§ 1519, 1520. This language is extremely broad and has not yet been tested.

Because virtually all companies have automatic deletion policies for e-mails and other electronic documents, the company must ensure that such policies are suspended. In addition, because many electronic documents may exist only on back-up tapes that are routinely reused and overwritten, the company must takes steps to take existing backup tapes out of service and preserve them in a secure location. As a result, one should take the following steps:

- The IT Department should be contacted and directed to suspend automated deletion processes and, instead, preserve e-mails for relevant employees during the period that relates to the allegations. Many companies have instituted policies of automatic purging of e-mail in-boxes, sent mail, and deleted items to conserve server space. The IT Department should be instructed to suspend those policies for existing e-mail files pending negotiation with the government. Alternatively, the IT Department can be requested to image the e-mail server, but defense counsel must ensure that the image includes sent mail and deleted items.

- Most companies use their backup tapes for disaster recovery purposes only – in other words, they use the backup tapes as a hedge against active servers being wiped out. That means that they rotate their backup tapes, often keeping 21 days of tapes that are continually overwritten. As a result, one of the first steps after receipt of a subpoena should be to take the backup tapes out of service and preserve them for later restoration and review.

- Hard drives and network drives of relevant employees should be imaged (being sure, of course, not to violate any data privacy laws).

In addition, after defense counsel gets involved, he or she should ensure that other possible sources of data – such as from consultants, agents, or other third parties over whose documents the company may have custody, possession, or control – are captured before being erased in the ordinary course.

A thorough collection and production process under the direction of outside counsel should follow quickly after a document retention communication has been sent out. A fair and reasonable interpretation of the text of the subpoena should be made so that potential sources of responsive documents can be identified and searched. Again, the company should generally resist the temptation to provide overly technical interpretations to subpoena language as might be done with a civil discovery request. Outside counsel will be able to help in this process by directly negotiating with the government regarding the scope of the subpoena and the date when such documents will be produced, as well as clearing up any potential confusion created by the drafting of the subpoena.

The production process should include the copying and Bates numbering of all documents, including electronic records, as well as a substantive review of the content of the produced documents so that the company and outside counsel can assess the potential areas of investigation and exposure to the company. During the collection process, privileged documents should be separated out and a log explaining the basis of the privilege being asserted should be

drafted and provided to the government. Failure to properly identify and segregate privileged documents can lead to unintentional production of such materials and claims of waiver. Inadvertent production can have drastic consequences, including possibly preventing the company from asserting privilege for any document that relates to the subject matter of the improperly produced document.

Subpoenas will often require the production of documents that contain a company's trade secret, proprietary, and/or confidential information. Although documents provided under a grand jury subpoena are protected from disclosure by the government by Fed. R. Crim. P. 6(e), the government may seek to show sensitive documents to employees of competitors during interviews. Similarly, documents provided under an administrative subpoena are not subject to Rule 6(e). As a result, it is important for counsel producing documents to mark appropriate documents as "Trade Secret/Confidential" and put the government on notice that the company is claiming the protections of the FOIA exemption for trade secret, proprietary, and/or confidential information 5/ and of 18 U.S.C. § 1905. 6/ In some cases involving highly sensitive information, the government will agree to a protective order.

B. Negotiating the Subpoena

Government subpoenas are often written to be extremely broad and, if complied with literally, would impose an enormous expense and burden on the company. Typically, government subpoenas now include detailed instructions for the production of electronic evidence. An example of such instructions can be found at Attachment 2. As a result, it is incumbent upon counsel to negotiate the scope of the subpoena with the government. In order to do so, however, counsel must have a thorough understanding of the potentially responsive electronic documents.

First, counsel should gain a thorough understanding of the electronic documents that the companies generate and retain that will be relevant to the inquiry and the storage media used to preserve them. This is actually a multi-step process. Initially, counsel must learn enough about the types of documents that exist to narrow the subpoena to a manageable scope through

---

5/ The Freedom of Information Act, 5 U.S.C. § 552(b), exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential."

6/ Section 1905 provides, in pertinent part:

> Whoever, being an officer or employee of the United States or of any department or agency thereof, . . . publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.

conversations and/or interviews with company employees. (In learning about the types of documents that exist, counsel must also learn about the company's sensitivities to producing such documents for such reasons as confidentiality and trade secret protection.)

Second, counsel should negotiate with the government to narrow the scope of the subpoena. For electronic documents, there can be several significant parameters. One, companies may have a significant number of backup tapes because there may be many e-mail or document servers or because other litigation may have precipitated a more expansive litigation hold. The backup tapes may be in different formats, which can add to the expense and time needed to restore them. And the backup tapes may be "full" backups of the system and/or "incremental" backups of new material since the last backup. In cases where there the backup tapes cover a long time period, the government may be amenable to a periodic restoration.

Two, the backup tapes and material resident on the servers will contain e-documents relating to many departments and employees that have no relation to the government's investigation. The government will often agree to limit the e-document production to particular departments or employees, which will reduce the quantity of data that must be reviewed during the discovery process.

Third, defense counsel should consider proposing a list of search terms to the government. These search terms can be used as an initial filter to screen out irrelevant e-documents and provide a set of documents for review for responsiveness to the subpoena.

While undertaking the steps discussed above, counsel will need to work on the third aspect of the case: preparation of the company's defense for an eventual presentation to the government.

C. E-Document Collection and Review

Backup Tape Restoration and E-Document Processing. There are three basic steps to restoring backup tapes to produce usable data that can be reviewed for production: restoration of the tapes to their original environment (such as Word, Outlook, or LotusNotes); de-duplication of redundant data and elimination of program files; and extraction of relevant data. The vendor may charge based on the total quantity of data restored, or may limit charges to usable data only. An example of a vendor's proposal to restore backup tapes is enclosed as Attachment 3.

If documents are being scanned and loaded into a discovery database such as Concordance or Summation, defense counsel will likely be able to create certain fields to track this information, but will need to work with a copying/scanning vendor to capture and record this information before beginning. Here, good planning is essential.

Before committing to a protocol, it is often useful to consult document database companies or litigation support consultants – either within a law firm or for hire. These experts should be able to identify and recommend best practices, and should be able to make suggestions that are separately tailored to hard copy documents (for which data will have to be supplied) and electronic data (for which metadata already exists). Such IT experts should also work with company IT personnel to make sure "forensic" copies of documents are made – *i.e.*, copies that

do not alter, but rather preserve the existing metadata on electronic files and that preserve the unallocated space on hard drives that contains documents that have been deleted but not overwritten.

Note that documents can be scanned and stored in a variety of formats: TIFF, PDF and JPG are the most common. Different document management systems use different formats and each has its own advantages and disadvantages. Defense counsel should consult with IT experts to determine which format and system will best meet his/her needs and budget. Also, if the client may later need to produce the documents to a regulator, it is often useful to make sure that the documents are scanned and stored in a format that the regulator prefers and contain metadata that the regulator requires to avoid additional expense in the future.

E-Document Review. If the document population is large as is almost inevitable in any investigation of a company, defense counsel will likely need to rely on a team of temporary attorneys to do an initial review of the documents to help defray costs. Here again, it is essential that the defense counsel plan the contours of the process as soon as possible. If documents have been loaded on to a database, the choice and clarity of the "tags" that reviewers will use to identify whether the documents relate to key witnesses or issues – or are privileged – will be critical to efficiency and effectiveness of the review process. An example of a coding sheet used by temporary attorneys is enclosed as Attachment 4. A regular member(s) of the defense counsel's team should train reviewers and answer questions as they arise to make sure all important information is captured. In addition, defense counsel must be sure to conduct quality control checks by reviewing documents marked for production by the temporary attorneys for responsiveness and privilege.

D. International E-Records and Data Privacy Issues

In the event that the government has a legal basis to require the production of evidence from a company's locations outside the United States, defense counsel must give consideration to data privacy laws in both the country of the relevant employees' residence and the country in which the relevant server is located. The European Data Protection Directive, adopted by the European Union in 1995, imposes wide ranging obligations regarding the collection, storage, and use of personal information relating to employees and customers. The measure, which has been implemented in each of the 18 member states of the European Economic Area ("EEA"), regulates both European business and the European subsidiaries of U.S. and other non-EEA corporations. Those companies are now required:

- to implement policies and practices that provide adequate protection for the privacy of the personal information held by that company -- both in the EEA and the US or any other non-EEA country to which personal data may be transferred for review or storage;
- to register with a national data protection authority and provide details of privacy protection practices;
- to give employees access to their personnel records;

- to place notices on a range of corporate documentation to give customers, employees and any other person from whom they collect personal information regarding their data practices; and
- to enter into data protection agreements with any third-party with whom employee or customer information may be shared.

The Directive also imposes an obligation on companies not to transfer personal data from their operations within the EEA to their operations in the United States (and other places outside the EEA) unless the recipient in the non-EEA country provides "an adequate level of protection" for the data. U.S. companies may comply either by participating in the Safe Harbor scheme administered by the United States Commerce Department or by the use of an intra-group agreement governing the flow of data across borders. An overview of the Safe Harbor principles can be found at http://www.export.gov/safeharbor/sh_overview.html. The Directive may necessitate the negotiation of an agreement with the government agency issuing the subpoena to assure "an adequate level of protection" for the data.

III. CONCLUSION

E-document discovery in criminal cases almost invariably involves significant expense for the client and resource consumption for defense counsel. The steps suggested in this article will not change that, but I am hopeful that they will help make the process more efficient and cost-effective.

Attachments –

- 1: Document Retention Policy Suspension Order
- 2: Instructions from GJ subpoena re: electronic evidence/document definition
- 3: Coding sheet
- 4: Coding and scanning proposal

ATTATCHMENT 1

DOCUMENT RETENTION POLICY SUSPENSION ORDER

TO: [Insert departments/company business units]

FROM: Office of General Counsel

DATED: [Insert]

[In accordance with the Company's {insert name of document retention policy}, this Suspension Order is being issued at the instruction of the General Counsel's Office.] Effective today, you should retain any and all documents (electronic and hard copies) and e-mails and attachments within these dates in any way related to [insert description] until further notice. All such records are suspended from disposition and shall not be destroyed under any circumstances.

It is extremely important that any document relating to the [insert description] be retained. Do not destroy or dispose of any material relating to [insert description], whether contained in a hard copy of the document, on e-mail, on a hard-drive or computer diskette, or in any other storage media, and whether a draft, a final, or even a duplicate copy of a document. If you have any questions about whether a document should be retained, please contact [insert name], [Company] General Counsel, at __ as soon as possible.

This Suspension Order supersedes all existing instructions with regard to the Company's records retention policies and will remain in force until further notice.

Thank you for your cooperation and assistance.

CERTIFICATION OF COMPLIANCE WITH

DOCUMENT RETENTION POLICY SUSPENSION ORDER

TO: Office of General Counsel
FROM: [Insert name]

I hereby certify that I have received a copy of the Document Retention Policy Suspension Order dated [insert] and that I will comply with it. I further certify that I will advise [the Office of General Counsel/Chief Compliance Officer] if I become aware of any instances in which I or anyone else fails to comply with that Order.

Signed: _____

Name: _____

Dated: _____

ATTACHMENT 2

INSTRUCTIONS

A. Scope of search. This subpoena calls for all documents in the possession, custody, or control of the Companies, as defined above, including but not limited to the possession, custody, or control of their officers, directors, employees, agents, attorneys, consultants, and contractors. The Companies are required to search all files reasonably likely to contain responsive documents, including but not limited to files left behind by former officers, directors, agents, and employees.

B. Relevant time period. All documents requested herein refer to January 1, 1999 to the present, unless otherwise indicated, and shall include all documents that relate to such period even though prepared or published before that period.

C. Privileges and Protections. Where a claim of privilege or protection is asserted in response regarding any document requested by this subpoena, and such document, or any part thereof, is not produced on the based of such claim, for each document or part thereof that is not produced, please provide a privilege log wherein you identify the type of document being withheld (e.g., letter, memorandum, handwritten notes, marginalia, etc.), a description of its contents, its author(s), all actual and intended recipients of the document, its date, and the specific privilege or protection being asserted, all with sufficient particularity as to allow the United States Attorney's Office and potentially a Court to assess the validity of the claim of privilege and/or protection.

D. Optional Production: In lieu of producing certain documents, you may, with -- and only with -- the specific and prior written consent of the U.S. Attorney's Office, submit a list, chart, or table showing the information requested, along with a certification from an officer of the Company(ies) attesting that the list, chart, or table is an accurate presentation of the information represented and requested.

E. Electronically stored information. If any document called for by this subpoena exists as, or can be retrieved from, information stored in computerized form, then you are directed to produce the document in computerized form, including sufficient identification of the applicable software program to permit access to, and use of, the document.

F. Conjunctions. The words "and" and "or" should each be read in the conjunctive and disjunctive (i.e., "and/or").

G. Tenses. Verbs used in the past tense should be read also to include the present tense, and verbs used in the present tense should be read also to include the past tense.

H. Singular/Plural: The singular number of a noun, pronoun, or verb should be read also to include the plural, and the plural number of a noun, pronoun, or verb should be read also to include the singular.

I. Manner of production. All documents produced in response to this subpoena shall comply with the following instructions:

(a) The Companies shall conduct their searches for responsive documents in a manner sufficient to identify the source and location where each responsive document is found.

(b) All documents produced in response to this subpoena shall be segregated and labeled to show the document request to which the documents are responsive and the source and location where the documents were found.

(c) To the extent that documents are found in file folders and other similar containers that have labels or other identifying information, the documents shall be produced with such file folder and label information intact.

(d) To the extent that documents are found attached to other documents, by means of paper clips, staples, or other means of attachment, such documents shall be produced together in their condition when found.

(e) All documents provided in response to this subpoena are to include the marginalia and post-its, as well as any attachments referred to or incorporated by the documents.

(f) In the event that there are no documents responsive to a particular request in this Schedule A, please specify that the Companies have no responsive documents.

(g) If documents relied upon or required to respond to any of this subpoena, or requested documents, are no longer in the possession, custody, or control of the Companies, the Companies are required to state what disposition was made of such documents, including identification of the person(s) who are believed to be in possession or control of such documents.

(h) Electronic media:

1. To the extent that the documents that are responsive to this subpoena may exist on electronic media, we are requesting that these documents be provided in the original manner in which they were stored. Each computer data tape must be labeled with the following information for each file contained on the tape:

a. File name(s);

b. Format (i.e., Extended Binary Coded Decimal Interchange Code (EBCIDIC), American Standard

8

Code of Information Interchange (ASCII));

c. Record length in bytes;

d. File blocking factor;

e. Indicate fixed length records;

f. Total file size in bytes;

g. Check total ("hash total"), field name, and figure.

2. The documents to be provided are the original computer data in the manner in which it was originally stored; however, in lieu of the original computer data media, the information may be provided on Compact Disk -- Read Only Memory (CD-ROM). If CD-ROM is chosen in lieu of the original computer media, it will conform to the following parameters:

a. Adhere to International Standards Organization (ISO) 9660, as information will be reviewed on an MS-DOS-based computer system;

b. ASCII format;

c. Fixed length record files (referred to as "flat files"), with each record to have the same length in a file. Each data field will have the same starting position, field length, and format between records.

d. Non-labeled files will be identified as such.

3. Each CD-ROM must be accompanied by an index containing the following information:

a. File name(s);

b. Format (i.e., EBCDIC, ASCII);

c. Record length in bytes;

d. File blocking factor;

e. Indicate fixed length records;

9

f. Total file size in bytes;

g. Check total ("hash total"), field name, and figure.

4. You are directed to convert fields to simple alphanumeric or numeric format as appropriate. Unpack fields, e.g., change packed decimal fields to unpacked numeric fields.

5. Multiple files may be put on one CD-ROM, however, only files pertaining to the same year should be placed on one disk.

6. You are to provide any and all correspondence or documentation to support the accurate conversion and analysis of the Electronic Data Processing (EDP) data, to include, but not be limited to, any and all internal operating instructions, computer software manuals, memoranda, notes, desk logs, computer files and computer hardware operating manuals, that contain the following:

a. Record layout with file descriptions (FD) (if files were created in a Common Business Oriented Language (COBOL) program).

b. Minimum Systems Documentation (including any system flowcharts and narrative system descriptions).

c. Data Dictionary or similar document, which defines the data elements in the record and defines the values and codes that can be contained in data elements.

d. Data set name of the file(s).

e. Record length.

f. Format of numeric fields.

g. Type of file, e.g., flat/sequential file, database file, Information Management System, Database Management System.

h. Type density in bits per inch.

i. Block size.

j. Make, model, and configuration of the computer system(s) that was/were used to make or compile the electronic date files.

k. Operating system, version(s), and platform used when EDP data was generated.

l. All versions of software used to transfer files onto computer tape, and the effective dates when/if software versions were changed.

11

HOGAN & HARTSON

ATTACHMENT 3

Coding Sheet

<table>
<tr><td>B.1 For each person identified in response to Paragraph IV.A.3:</td><td></td><td>Time period: January 1, 1999 to July 2005</td><td></td><td>Geographic area:</td><td></td></tr>
<tr><td rowspan="2">(a) All calendars, appointment books, address books, rolodexes, diaries, notepads, business card files, PDA files, or any similar documents relating to or recording such person’s daily activity, including such records maintained on computers or PDA (e.g., Palm Pilot), with the user of each item identified where not self evident;</td><td rowspan="2">☐</td><td rowspan="2">C.1 Contracts and Agreements with Suppliers. All documents relating to actual or proposed agreements, meetings, visits, discussions, conversations, telephone calls, facsimiles, written correspondence, or other communications (whether formal or informal, business or social) between any officer, director, agent or other employee of your Company and any officer, director, agent, or other employee of any other Supplier relating to or affecting the prices, discounts, market strategies, bids, proposals, quotes, or other terms or conditions for Supply Contracts.</td><td rowspan="2">☐</td><td>C.5 Recorded Conversations. Any audio and/or video recordings relating to Supply Contracts and involving persons identified in Paragraph IV.A.3.</td><td>☐</td></tr>
<tr><td>C.6 Directories. Each internal directory, personnel directory or listing, and corporate organizational chart or table prepared by your Company.</td><td>☐</td></tr>
<tr><td>(b) All documents relating to business travel and entertainment incurred by such persons, including documents reflecting your Company’s reimbursement of such expenses;</td><td>☐</td><td rowspan="2">C.2 Gifts. All documents that record, refer, or relate to any gift, entertainment, gratuity, remuneration, or payment made, or expense incurred, regardless of nature or form, by, or on behalf of your Company or any officer, employee, or agent or representative of your Company, directly or indirectly to or for:
(a) any person responsible for preparing requests for proposals, quotes, or bids for any public entity; or
(b) any person respsonsible for awarding or executing any contracts, subcontracts, or purchase orders in connection with any proposals awarded or funded by any public entity.</td><td rowspan="2">☐</td><td>C.7 Batch Tickets. All batch tickets generated during the subpoena period.</td><td>☐</td></tr>
<tr><td>(c) All documents that refer or relate to telephone calls and facsimile transmissions made or received by such persons, including any residential telephone bills for which your Company paid or provided reimbursement; and</td><td>☐</td><td>D. All original documents relating to bids, proposals, prices, price quotes, and negotiations for, and the awarding of Supply Contracts during the subpoena period, whether or not awarded to your Company, including but not limited to:</td><td></td></tr>
<tr><td rowspan="2">(d) All personnel files and records.</td><td rowspan="2">☐</td><td rowspan="3">C.4 Annual Reports and Financial Statements. All of your Company’s annual reports and financial statements, including, but not limited to: balance sheets, annual statements of profit and loss, income statements, statements of financial position, management letters from accounting firms, and reports made to shareholders, owners, or major creditors.</td><td rowspan="3">☐</td><td>D.1. Announcements of Supply Contract bid lettings;</td><td>☐</td></tr>
<tr><td>D.2. Requests for specifications, proposals, or quotes for Supply Contracts;</td><td>☐</td></tr>
<tr><td></td><td></td><td>D.3. Bid or bidder lists for Contracts;</td><td>☐</td></tr>
</table>

D.4. Documents submitted for the purpose of pre-qualification in Supply Contracts;	☐	D.8. Worksheets, spreadsheets, reports, takeoffs, markup calculations, pre-bid cost estimates, bid preparations, computations of expected or actual profit or loss, and any other documents used in whole or in part in determining the amount of the bid or quote submitted or proposed to be submitte by your Company in connection with a Supply Contract;	☐	D.12. All documents relating to or recording any actual or proposed changes in price, discount, or other terms or conditions for Supply Contracts during the subpoena period;	☐
D.5. Bids, quotes, proposals, price lists, or other documents setting forth your Company's or any other Supplier's proposals or prices;	☐	D.9. Documents relating to the formulas, procedures, or other means and methods by which you determine or determined costs, markups, bids, quotes, prices, or terms and conditions in connection with a Contract;	☐	D.13. Supply Contracts, including those projects for which your Company acted as a subcontractor; and	☐
D.6. Affidavits or certificates of non-collusion or independent price determination for Supply Contracts;	☐	D.10. Pre-bid or pre-quote letters, memos, and other communications between your Company and any other Supplier, customer, or prospective customer regarding any Supply Contract;	☐	D.14. Invoices for work performed in connection with a Contract.	☐
D.7. Documents <u>not</u> sent to customers or prospective customers, setting forth your Company's or any other Supplier's estimates, bids, quotes, proposals, or prices for Supply Contracts;	☐	D.11. Memoranda, notes, messages, letters, electronic mail, and other communications, computerized and otherwise, sent and/or received by employees of your Company regarding the determination of the bids, quotes, and prices submitted or proposed to be submitted by your Company in connection with Supply Contracts;	☐	Archive Box Number: _____ Doc Date: _____/_____/_____ Author: _____ Doc. Title: _____	

1st Rev: _____

Rev. Date: _____

2nd Rev: _____

Rev. Date: _____

Names Mentioned:			**Other Companies:**
☐ John Doe A	☐ John Doe F	☐	Company A
☐ John Doe B	☐ John Doe G	☐	Company B
☐ John Doe C	☐ John Doe H	☐	Company C
☐ John Doe D	☐ John Doe I		
☐ John Doe E	☐ John Doe J		

ATTACHMENT 4

ASSUMPTIONS

- Data is stored on roughly 100 DLT tapes.
- Data will put through EDD processing.
- Data will be culled by de-duping globally across all of the data set.

SOLUTION

- Technical staff will restore DLT tapes to network.
- All electronic data restored will be processed, de-duped globally, text extracted, metadata extracted and delivered in a Concordance database with links to native files.
- Will deliver data on a rolling basis.
- Will be prepared to tiff responsive docs on a total or rolling basis for production purposes.

PRICING

Will bill based on the method least expensive method.

DLT / LTO Restoration & EDD Processing billed on responsive GB count

Per Unit	Unit	Service
$ 215.00	Tape	DLT or LTO Tape Restoration
$ 800.00	GB	EDD Processing and Deduping to Native File
$ 475.00	GB	EDD Processing to Tiff Image
$ 0.01	Image	Branding
$ 0.05	Page	Blowback w/ slipsheets
No Charge	HD / CD / DVD	Delivery Media w/ Load File

Or

DLT / LTO Restoration & EDD Processing billed on total GB count

Per Unit	Unit	Service
$ 215.00	Tape	DLT or LTO Tape Restoration
$ 125.00	GB	EDD Processing and Deduping to Native File (1 - 50 GB)
$ 65.00	GB	EDD Processing and Deduping to Native File (51 - 100 GB)
$ 25.00	GB	EDD Processing and Deduping to Native File (101+ GB)
$ 475.00	GB	EDD Processing to Tiff Image
$ 0.01	Image	Branding
$ 0.05	Page	Blowback w/ slipsheets
No Charge	HD / CD / DVD	Delivery Media w/ Load File