ESI DEMYSTIFIED

Streamlining the E-Discovery Process Through Internal Processes and Controls

Melinda Burrows
Bruce Cosgrove*

The widespread proliferation of electronically stored information (so-called ESI) has transformed the rules of engagement for those who litigate. The risks inherent in electronic data management are many; one of the most challenging things to manage is actually knowing what you have and where to find it. These materials will focus on practical tools for creating a process to identify, locate and collect ESI in the context of an investigation, subpoena, lawsuit or government request—what’s become fondly known as “E-Discovery.”

The Rule 26 Amendments May Not Be So Bad

Much has been made of the way in which December 2006 changes to the Federal Rules of Civil Procedures have created new, more onerous obligations for litigation counsel. Despite the hype, counsel and their clients have nothing to be afraid of—at least not if they prepare.

Following the 2006 amendments, E-discovery, at least in federal court, may in many ways be easier. The changes to the rules inject reasonableness and accessibility considerations into the E-discovery process. Rule 26(f)’s requirement that counsel meet and confer regarding E-discovery issues no more than 100 days after a complaint is served presents an opportunity for the parties to streamline discovery efforts and disputes early in the process. While many state court systems have not wrestled with E-discovery issues as extensively as the federal courts, state courts may look to the federal courts’ evolving expertise in this area to fill the vacuum.

Leverage the Rules to Proactively Prepare for E-Discovery

Proactive internal and external counsel have used the amended federal rules as a launching point for the creation of internal E-discovery processes. A thoughtfully designed electronic data collection process is a sound investment in litigation risk and related cost management. The development of a process will:

(1) establish a partnership between information technology (IT) and legal professionals before a crisis;

(2) create a system that effectively leverages internal resources by de-mystifying the IT system and retrieval process; and

*Melinda Burrows and Bruce Cosgrove work in the Legal Department at Progress Energy Service Company, LLC.
(3) ensure that external resources, including outside counsel, are used productively and cost-effectively.

**Step 1 – Locate Your Data**

The creation of an E-discovery process may sound like a daunting prospect, but it doesn’t need to be. In fact, the point of creating the process is to simplify and streamline data identification, collection and retrievability. The key to creating a defensible process is to understand up front where and how your company stores data—so-called data mapping. While data mapping requires an up-front investment of IT resources, this investment may pay off in a single lawsuit if it staves off a spoliation claim.

**Step 2 – Create a Process That Will Identify, Preserve and Collect ESI**

Once an organization understands where its electronic data resides, a process can be created that allows for the timely protection and retrieval of relevant data in response to a litigation hold. An effective and defensible process should be routine, repeatable, user-friendly, scalable and auditable.

At a minimum, an E-discovery process should include the following steps:

1. directions on issuing a litigation hold that includes notification to data custodians and internal IT resources to preserve paper documents and ESI;
2. directions for identifying and communicating with document custodians,
3. directions for collecting ESI; and
4. defined roles and responsibilities for legal, IT and client stakeholders.

Process attributes particular to a specific organization will be driven by a number of factors, including the size of the organization, the complexity of its electronic data systems and storage, the type of data stored and the frequency of litigation.

**Forms and Checklists May Streamline the E-Discovery Process**

The materials that follow have been adapted from an E-discovery process developed for a mid-sized company and are intended to guide counsel through the workings of an internal E-discovery system. The forms and checklists may be customized for use by a particular company or used as a frame of reference for creating a unique process. These documents may serve to develop the framework for an audit trail and as evidence that a company exercised reasonable, good faith diligence to identify and preserve ESI.
Dispute Process Checklist (Tab A) – This document creates a base line road map and audit trail for the e-discovery process. It provides step by step instructions, identifies responsible parties, and requires dated sign-offs at critical times.

Protocol to Identify Custodians (Tab B) – This document outlines multiple ways to identify potential data custodians and data repositories to ensure that the organization exercises sufficient diligence when issuing a litigation hold.

Sample Hold Notice (Tab C) – This document is intended for distribution to potential data custodians as soon as possible after identifying the need for a litigation hold.

IT Checklist (Tab D) – This document is intended to track the due diligence of a litigant’s internal IT resources. It puts a company’s IT department on notice of pending litigation and provides step-by-step instructions intended to ensure that ESI subject to a litigation hold is adequately secured. It requires sign off by IT personnel indicating receipt of the litigation hold notice and provides a menu of options from which legal resources may select the data to be secured.

Initial Contact Form and Interview Checklist (Tab E) – This document provides an outline for interviews with data custodians. The form allows legal personnel to document information obtained during the interview, creating an audit trail for the company’s diligence efforts.

Collection Agreement Form (Tab F) – This document is a checklist for data custodians. Custodians are asked to sign the document, indicating that they have, to the best of their ability, provided assistance in searching for data subject to a litigation hold.

Duty to Retain and Preserve Reminder for Document Custodians (Tab G) – This document may be provided to data custodians either at the time a litigation hold is issued, or during the custodian interview. It clearly and simply outlines the company’s duty to identify, preserve and collect data potentially relevant to a pending matter.

Glossary Terms (Tab H) – This document is a quick reference guide for those new to E-discovery. It provides clear and concise definitions of terms commonly used in discussing issues relating to ESI.

Conclusion

ESI, and the discovery challenges it presents, are here to stay. Proactive companies and their counsel may be well advised to get in front of E-Discovery issues so that when faced with a lawsuit or other data request, that request may be turned around with a minimum of disruption, cost and overall risk. An upfront investment in data mapping and process development may pay off for years to come.
Dispute Process Checklist

1. Determine need for litigation hold and designate discovery liaison.
   Date: __________________________
   Responsible Party (RP) may include an individual in the Legal Department as well as outside counsel, vendors and/or consultants retained to assist in the matter and serving under the general direction of the Legal Department.
   RP: __________________________

2. Identification of individuals/organization to receive Hold Notice.
   Date: __________________________
   RP: __________________________

3. Initial Hold Notice sent.
   Date: __________________________
   RP: __________________________

4. IT Department acknowledges receipt of Hold Notice.
   Date: __________________________
   RP: __________________________

5. Discovery liaison acknowledges receipt of Hold Notice.
   Date: __________________________
   RP: __________________________

6. IT Department contacts discovery liaison to discuss IT security checklist
   Date: __________________________
   RP: __________________________
   STEPS 3 – 5 SHOULD BE COMPLETED WITHIN ONE BUSINESS DAY OF LITIGATION HOLD DETERMINATION.

7. Attorney/discovery liaison follow-up with IT Department to clarify procedure to be utilized in electronic discovery.
   Date: __________________________
   RP: __________________________

8. Discovery liaison opens Process Notebook. Notebook is to capture and record all activities of production cycle, date(s) of activities and persons performing activities. Process Notebook includes this checklist.

9. Discovery liaison to follow up on feedback from Hold Notice. New custodial names from feedback immediately sent Hold Notice. Repeat Steps 3 through 8. Repeat Step 8 as often as necessary. See Step 10. Discovery liaison sets Outlook calendar to also auto-remind to periodically alert hold notice recipients that the hold notice remains in effect. Schedule of these notices to be determined by counsel.
   Date: __________________________
   RP: __________________________

Date: _________________________________________
RP: __________________________________________
10. Legal Department (discovery liaison or other designee) follow-up with recipients of Hold Notice. Schedule/conduct interviews. Use Contact Form for each contact. Step 9 may be an ongoing process. Contact forms must be compared against Hold Notices and feedback from recipients of Hold Notices.

   Date: _______________________________________
   RP: _______________________________________

11. Discovery liaison to set Microsoft Outlook Calendar to auto-remind regarding litigation hold (daily, weekly, monthly, quarterly, etc. depending on complexity of matter). Liaison to send out additional Hold Notices and repeat Steps 3 through 5. Auto-remind should also be set to remind liaison to follow-up on Contact Form issues.


   WHEN POSSIBLE, STEPS 11-13 SHOULD BE COMPLETED IN ADVANCE OF MEET AND CONFER.

<table>
<thead>
<tr>
<th>ID No.</th>
<th>Custodian</th>
<th>Date</th>
<th>Location</th>
<th>RP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Date: ________________
   RP: ________________

13. Collection of ESI from custodians by IT Department. Discovery liaison provides instructions on specific material to gather.

14. Transfer of electronic data by IT Department to Legal Server. Transfer should retain custodian identification. Transfer includes Chain of Custody Log. Log should be maintained from this point forward by discovery liaison. Chain of custody to capture any movement of data including to vendors and outside counsel. Vendors must be qualified for compliance with chain of custody and provide secure IT and physical environment.

15. **Decision Point:** How will electronic data be reviewed?
   Decision reached: Decision recorded in Process Notebook.
   Date: __________________________
   RP: ___________________________

Tab A
Is conversion necessary?  
What in-house tools are available?  
Outside counsel preference  
Provide data to “qualified” vendor  
Convert to hard copy (advance to Step 20)

16. Type of electronic review chosen
   - [ ] Key word search
   - [ ] Comprehensive review
   - [ ] Other

   Date: _________________________________________  
   RP: __________________________________________

17. Electronic Data Segregation. Standardized production sorts listed below.  
Utilize electronic tagging methods in tandem with sorts to build collection for each category below:

   **Responsive not Privileged:** For all documents which are responsive, apply unique electronic Bates number. Responsive data will include material which may ultimately be excluded from production but that must be accounted for at some time throughout the process.

   **Responsive and Potentially Privileged:** This sort is to remove Bates numbered data that is identified as potentially privileged. Remove this data from responsive sort. It will be necessary to have a final definitive review to determine privilege status. Enter privileged material on privilege log. Produce material initially withheld as potentially privileged that ultimately is deemed not to be privileged.

   **Proprietary:** This sort to remove proprietary data from Responsive not Privileged sort. Follow guidelines for handling proprietary data per Section 12. This material may be produced at a later date. Auto-remind to produce.

18. Collection of hard copy

   Convert hard copy to electronic
   - [ ] Yes: Go to Steps 14/15
   - [ ] No: Go to Step 19

   Date: _________________________________________  
   RP: __________________________________________

20. **Decision Point:** Hardcopy production scope  
    Produce on document level.  
    Produce on file level.  
    Bates number responsive material.  
    Remove potentially *privileged* material.
Proprietary: Remove from production. Proprietary data will be produced when appropriate.

Date:__________________________________________

RP:___________________________________________


Electronic – electronic media.

From sort Responsive not Privileged create a minimum of two identical sets of data. One set may reside as tagged or in a unique database on litigation support software. Transfer one (or both if not utilizing litigation support software) to electronic media (CD, DVD, jump drive, removable hard drive) for eventual production.

Date:__________________________________________

RP:___________________________________________

Hard Copy.

Maintain record or physical copy of (1) all documents produced and, (2) all documents designated for copying.

Date:__________________________________________

RP:___________________________________________

22. Resolution of Matter.

Determination as to whether records may be destroyed or otherwise released. Are the records responsive or otherwise related to any other ongoing matters? Send out notice to Legal Department.

☐ Yes – Preserve data and consult with discovery liaison

☐ No – Proceed to Step 26, Notification Lifting Hold Notice

23. Notification Lifting Hold Notice.

Notification Lifting Hold Notice sent immediately after resolution of Step 21 above and authorization. Notification sent to all recipients of Hold Notice (including cc) and those listed on Contact Forms.

Auto-alert set by discovery liaison to periodically remind liaison that when matter has been resolved, notification must be sent.

Destruction of records/data compiled and produced. Destruction consistent with corporate guidelines.

Date:__________________________________________

RP:___________________________________________


Date:__________________________________________

RP:___________________________________________
Protocol to Identify Custodians

The identification of custodians of potentially relevant records and other data generally relies upon the following:

- **Corporate knowledge:** Corporate knowledge is the knowledge of those most familiar with the dispute. These are generally the first people the Legal Department is likely to associate with the dispute. Contacting these employees and initiating discussions both with them and their management will likely produce the most critical players in any dispute. Corporate knowledge can also be defined as those with a history of the relevant events and players. Tapping into that history will provide additional names of relevant players. Corporate knowledge generally provides the first set of names for a hold notice.

- **Interviews:** Interviews, or discussions with those identified through corporate knowledge, should seek to further the list of potential custodians. Hold notices, interviews and other contacts should continuously seek to identify others who may have, or be aware of, data related to the dispute. Often the response one gets is that the only data others might have would be duplicative. In most cases duplicative information, especially in hard copy, is responsive. Often, if an individual was involved enough to have copies, he or she possibly was involved enough to have original material as well.

- **Records:** As hardcopy documents and ESI are collected, they should be reviewed for additional names. The additional names found on records serve both to widen the scope of individuals involved and to serve as an aid to assist in enhancing the recollection of those being interviewed. Identification of additional names from records may necessitate follow-up interviews. Equally important—it should be noted that opposing counsel will be reviewing the produced records for names to both identify potential players and to test the efficacy of the production.

- **IT Department:** The IT Department has access to all employee email. By leveraging this access with a variety of tools the IT department may be able to conduct key word or other searches against email. The IT department may also have similar tools which permit it to search against repositories of ESI.

Organizational charts, floor maps and headcount documentation are also useful records in identifying individuals who may possess potentially responsive material or facts related to the dispute.
Sample Hold Notice

We have received notice of potential litigation involving _____________. During the course of my investigation of this matter, it has come to my attention that you may have prepared, received, or otherwise control documents that are related to the matter. It is important that you maintain these documents and that you ensure that they are not destroyed. For the purpose of this request, “documents” includes both paper and electronic files. Examples of electronic documents subject to this request include but are not limited to: e-mail messages, attachments, Adobe Acrobat pdf documents, Microsoft Word documents, Microsoft Excel documents, Instant Messaging, web pages, meeting boards, tape recordings, voice mail and digital photographs. Documents include drafts, letters, memos, notes, calendars, expense accounts, revisions, reports and any and all other records created that may relate to the matter, as well as copies of those records.

Please notify me if you are aware of any other employee who is not on this distribution list but who may have knowledge concerning this matter, or possess or control any documents or records relating to the matter, whether or not those documents might be duplicates of documents others control. Please let me know immediately who that person is so that I may contact them as well.

I also ask that you let me know in the event that any employee you reasonably believe may have knowledge or documents relating to this matter should leave employment with the company, whether voluntarily or involuntarily, so that we may take the necessary steps in order to preserve the records and data of such person.

The company has an obligation to preserve any and all records and other data that may relate to this matter. Failure to do so can result in severe penalties to the company and may jeopardize our ability to resolve the matter in the company’s favor. A representative of the Legal Department will be contacting you soon to discuss the types of documents you may control and their relevance to the issue. That person will provide instructions on segregating and preserving the data as well as how that data may best be collected so as to minimize the impact of this matter on your day-to-day duties. New documents created that relate to this matter will also need to be protected and preserved. Until you have communicated with a Legal Department representative who can inform you as to the types of records which may be called for, you must suspend destruction of any records regardless of your interpretation of the relevance of those records.

Please feel free to contact me if you have any immediate questions or concerns.

Thanks very much for your help.
IT Checklist

Date: ____________
Initials: __________

1. IT has received notification of litigation ____________________.

2. IT has assigned (NAME) __________________________ as Legal’s contact for this matter.

3. IT has assigned (NUMBER) ___________ to this matter for its internal tracking purposes.

4. IT has initiated a Chain of Custody log to track all access, exchange and location of data until final closeout of the matter.

5. Please indicate on the checklist the course of action you are requesting from IT:

Schedule a meeting to discuss course of action:

Priority: 
☐ Meet today
☐ Meet as soon as possible
☐ Meet when convenient
☐ Discuss matter via telephone

Secure data for the persons identified with this matter:
☐ Immediately
☐ After feedback from Legal Department
☐ After meeting with responsible attorney

Data to be secured includes – check all that apply:
☐ PC hard drive
☐ Corporate applications (specify)
☐ Departmental database
☐ Shared drives
☐ U drive/G drive
☐ Voicemail
☐ Instant messaging
☐ Laptop
☐ External sources
☐ Other (list other locations)
Initial Contact Form And Interview Checklist

Person contacted:

Matter/Case Number:

Contacted by:

Date/Time:

Location:

Phone Number/Extension:

Means of contact (indicate all that apply): Voicemail Email Personal visit Phone

Successful Contact: ☐ Yes ☐ No

Repeated attempts to contact: Date/Time

Need to follow-up to collect data: ☐ Yes ☐ No

Interviewed by:

Checklist

Identify yourself and explain that you are following up on Hold Notice from counsel.

Describe nature of litigation or matter.

Describe corporate responsibilities to secure data and potential corporate liability for failure to do so. See Duty to Retain and Preserve.

Inquire into contact’s role in matter.

Explain steps already taken by IT:

- IT has been notified and is prepared to mirror hard drive and secure other ESI if necessary.
- You have temporarily been suspended from auto-delete functions the company routinely runs.

Tab E
Explain Collection Agreement Form which interviewee must execute regarding the information and assistance they provide.

Determine if this will be a self-search or Legal Department search.

Explain the types of ESI/hardcopy we must locate:

- **Hardcopy records**
  - Personal files
  - Departmental files
  - Off-site archives
  - Company business records that may not be under the company’s control
  - Printed emails

- **Electronic data from:**
  - Hard drive
  - Shared drives, other
  - Other applications
  - Departmental databases, electronic records storage (DocsOpen, etc.)
  - Flash USBs, CDs, DVDs, Diskettes, other storage media
  - Laptops, PDAs, Blackberry
  - Cell phone (photos, voicemail, text messages)
  - Instant Messaging
  - Home computer
  - Tape backups
  - External hard drives
  - Proprietary databases
  - Voicemail
  - Tape recording
  - Other

Are they aware of others who may have potentially relevant data? Explain that even identical copies of data may be responsive.

Schedule time for personal interview, if necessary, to review their filing systems and documentation.

Notify IT of this individual: □ Yes □ No

Did this individual furnish you with additional names of individuals who should receive a hold notice?

□ Yes: List names and other contact information if available. Notify discovery liaison to have hold notice generated, EAS suspended and IT Security informed.

□ No
If interview is in person, have interviewee execute Collection Agreement Form. If interview by phone or other means and no personal contact is anticipated, explain and send Collection Agreement Form. Set calendar to auto-remind that sent form is due back. Follow up as necessary.

Interview Notes:
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
Collection Agreement Form

I, (employee name and corporate id), confirm that for litigation matter (matter and case number), I have cooperated in good faith with the Legal Department and/or its representatives by providing them with personal knowledge and access sufficient to complete a thorough search of the following:

Hardcopy records, including, but not limited to:

- Personal files
- Departmental files
- Off-site archives
- Business records that are located elsewhere (home, etc.) not under the company’s immediate control

Electronic data, including, but not limited to:

- Hard drive
- Shared drives
- Applications
- Departmental databases
- Flash USBs, CDs, DVDs, Diskettes, all other storage media
- Laptop, PDA, Blackberry
- Cell Phone (photos, voicemail, text messages)
- Instant Messaging
- Home computer
- Tape backups
- External hard drives
- Proprietary databases
- Voicemail
- Tape recordings
- Any other data sources

To the best of my ability I have searched for, or assisted the Legal Department in its search for, all data relevant to the above matter. I have not deleted or modified any potentially relevant data since receiving the hold notice. In addition, I have provided the names of other individuals who may have data and/or knowledge of other locations where relevant data may be held.

I understand the importance of this matter, and have fully cooperated with the Legal Department and its representatives.

________________________________________   ___________________
Signature          Date

________________________________________   ________________________________
Printed name          Title and Department
Duty to Retain and Preserve

The company has a legal duty, obligation and responsibility to retain and preserve all potentially relevant electronically stored information (ESI) and hardcopy (paper) documents when litigation is reasonably anticipated. This duty includes identifying all sources of potentially relevant information likely to be requested during the legal discovery process. When an employee has received a litigation hold notice or has otherwise been alerted by the Legal Department of the need to preserve data, it becomes the responsibility of the employee to cooperate, collaborate and provide information to the Legal Department, or its representatives, to ensure that all relevant information is identified, preserved and retained. This duty extends to ensuring that no potentially relevant data under the employee’s custody or control are lost, altered or destroyed. If an employee has knowledge that ESI or hard copy documents have been intentionally or unintentionally destroyed or altered after the litigation hold notice has been issued, the employee should immediately contact the hold notice author or other appropriate Legal Department personnel.

Failure to comply with this obligation and with the procedures outlined in the hold notice could result in extreme penalties, judgments or sanctions against the company as well as personal or corporate criminal liability.

The company must take all reasonable steps to preserve potentially relevant data until the resolution of the matter. This includes both data created prior to the hold notice as well as data that continues to be created prior to the resolution of the matter. The employee will be notified by the Legal Department when the matter is resolved and when it becomes permissible to return to appropriate, routine data management practices.
Glossary Terms

**Chain of custody** – A process used to maintain and document the possession, movement and handling of evidence from the time it is obtained until it is presented in court. Documented chain of custody is used to prove that evidence has not been altered, tampered with, or otherwise modified.

**Concordance** – A widely-used litigation document management application. Corporate Legal Departments use both Concordance and its leading competitor, Summation, to manage data-intensive products. Most large law firms will have either Concordance or Summation, or both. Using the application that aligns with the company’s outside counsel will facilitate the transfer of data.

**Custodian** – Person having custody or control over hardcopy documents, ESI or other materials which may be relevant in a given matter. The custodian may be no more than an individual controlling his or her own material or an employee responsible for the maintenance and control of document repositories and/or ESI.

**De-duplication** – The electronic process of identifying, and removing or tagging identical duplicates within a data set of ESI. This process involves placing all the ESI into a single database and searching for duplicates. The parameters of de-duplication should be discussed during the 100 day meet and confer.

**Designate** – The act by one party of selecting hardcopy documents or ESI for copying or transfer from the opposing party.

**Drives** – The computer storage device found in PCs, servers and portable storage media.

**ESI** – Electronically stored information.

**External hard drive** – USB connected disk drive that resides in its own hard case. Often used for backing up or transferring large amounts of ESI.

**Flash USB** - See Thumb drive.

**FRCP** – Federal Rules of Civil Procedure.

**Hard drive** – The primary computer storage medium in desktop and laptop computers, it is physically located within the computer.

**Hold notice** – A communication issued as a result of current or anticipated litigation, investigations or other such matters that suspends the normal disposition of hardcopy records, ESI and other potentially relevant media.
**IT (Information Technology)** - A vital sectional or departmental group within most large organizations responsible for the maintenance of electronic hardware, software and data.

**Image** – The process of making an identical copy of a drive or other storage medium capturing all contents including file fragments, hidden files, deleted files, and empty spaces. Often referred to as mirror or mirroring.

**Keyword** – A word, term or a string of words designated by a user as important for conducting and limiting electronic searches.

**Metadata** – Data about ESI that captures ESI attributes describing the history of the data including name of originator, size, date, modifications, etc. Much of this data is not seen by the casual user but is likely to be relevant in discovery.

**Native File** – A file saved in the format of the original application used to create the file. Viewing or searching files may require the original application.

**Network share drive** – A storage medium which can be read and written to by a number of users.

**OCR (Optical Character Recognition)** - A process that translates and converts printed matter on an image into a format a computer can manipulate and “read” thereby making the matter text searchable.

**PDA (Personal Digital Assistant)** - A small hand-held, mobile computer that assists in a variety of business tasks. The PDA will “synch up” with the user’s primary computer transferring and receiving updated information.

**PDF (Portable Document Format)** - A proprietary format of Adobe Corporation. PDF has become the preferred method of transmitting or posting electronic documents that the sender does not want to be altered.

**Responsible party** – The employee or outside resource assigned the primary responsibility to perform and document a given task.

**Spoliation** – The intentional or negligent destruction of hardcopy records, ESI or other media which may be relevant to ongoing or anticipated litigation, investigations, audits or other such matters.

**Summation** – A litigation document management application. Summation and Concordance are the leaders in this field. Most large law firms will have either Concordance or Summation, or both. Using the application that aligns with the company’s outside counsel will facilitate the transfer of data.

**Tape back-up** – Magnetic tape for storing duplicate copies of hard disk files. Magnetic tapes are used by IT as part of the company’s centralized back-up management program.
**Thumb drive** – A removable ESI storage medium that connects to a USB port. Referred to as a thumb drive because it is approximately the size of a thumb. Often carried as a fob on a lanyard. Also referred to as a key drive or jump drive.

**USB** (Universal Serial Bus) – A hardware interface for attaching peripheral devices to a PC.

**TIFF** (Tagged Image File Format) - A widely used format developed in the early 1980s which results in what is essentially a picture of the document.

**Zip Disk** – A 3.5” removable disk drive.