Attachment 2
Questions About Electronic Systems and Back-up/Archiving Policies

1.   Computer Hardware, Systems, and Applications.

a.   What types of computers (e.g., mainframe, work stations, laptops) does the company have?

b.   What types and versions of operating systems (e.g., Windows, Linux, UNIX) does the company have on each type of computer? Which operating system is generally loaded onto employee desktops? Please specify all dates of major changes/upgrades.

c.   How many servers and what types of servers (e.g., exchange servers, e-mail/file servers) does the company have and where are they located (e.g., physical locations)?

d.   Do employees use laptops to conduct business? If so, how? How are the laptops connected to the network servers (e.g., remote access programs, synchronization procedures)? Who owns the laptops?

e.   Do employees use handheld devices (e.g., BlackBerrys, Treo smartphones, Palm Pilots) to conduct business? If so, how? Who owns the devices?

f.   Where do employees access and save documents (e.g., locally (c: drive), shared drives on the server, or a personal location on the server)?

g.   Which software applications are loaded onto employee desktop computers? Please note what is part of the standard load versus specialized applications that are loaded onto only a few employees' computers.

h.   Does the company use Instant Messaging ("IM")? If so, which IM application? How long are IM text messages retained by the company? Are employees allowed to use their own IM applications on the company's computers?

i.   Does the company use a central document management system (e.g., iManage, OpenDocs)? If so, which application? Which employees have access to it and what is stored on it? What is the company's archiving and/or retention policy with respect to documents stored in any document management systems?

2. E-mail System.

    a.   What e-mail system is in use at the company? When was it installed?

    b.   Where is employee e-mail stored for retrieval? On the company network? Does the e-mail stay in the network after the employee accesses it?

    c.   How long does the e-mail software allow employees to retain e-mails? Is there an auto-delete policy? If so, what time period is associated with this policy? Is there any other limit on e-mail retention (e.g., a megabyte limit)?

    d.   How is e-mail archived or backed-up?

    e.   Where else might employees store e-mail? Is there a procedure for saving e-mail, or does it depend on individual preferences?

    f.   What happens to e-mail retrieved on a laptop or PDA/Blackberry? Is it still available on the employee's desktop computer? How is e-mail on PDAs/Blackberrys stored? Where do employees store it? How long are e-mails on these devices retained by the company?

3. Back-up Procedures.

    a.   What are the types of back-ups performed (e.g., full back-ups, incremental back-ups)?

    b.   What types of data are backed-up (e.g., e-mails, word-processing documents) and which data is backed-up (e.g., e-mail servers, desktops)?

    c.   What type of media is used to store the back-up data?

    d.   What application is used to create back-ups?

    e.   What is the back-up schedule (e.g., each business day, weekly, monthly)? When are the back-up media recycled for reuse (i.e., overwritten)?

    f.   Which back-up media containing potentially responsive data were in existence at the time the Second Request was issued to the company?

    g.   Are back-up media individually labeled by type of data stored on the tape, or by employees whose data is stored on the tape?

    h.   Are back-up media indexed and/or logged by back-up software?

i. Has the company restored back-up tapes within the last two years, for any purpose, including for other litigation or to retrieve data inadvertently deleted from the company's computer systems?

j. Does the company use a remote, on-line back-up service to maintain and store the tapes?

k. What is the location of any and all back-up media, whether on or off-site?

l. Is there a disaster recovery policy for electronic files (e.g., what to do if data is lost after disaster such as a power outage, act of God)? If the disaster recovery plan is different from the regular back-up policy, briefly describe how it differs from the above answers about back-ups.

4. **Archival Data.**

a. What types of data are archived?

b. How are archived media labeled, indexed, and/or logged?

c. What type of media is used to store the archived data? Where is it located?

d. What application is used to create archives?

e. Has the company restored archived data within the last two years, for any purpose?

5. **Recent Merger/Acquisition.** Was any part of the company recently acquired or sold? If so, were back-up efforts made as the acquired company became integrated? In responding to this questionnaire, please account for and provide responsive information for any electronic systems that are still in use that may have been acquired as part of a merger or acquisition.

6. **Document Retention Policy.** Please provide a copy of the company's document retention policy, including any specific policy relating to electronically stored information.

7. **Databases.** (Note, this information may not be necessary for a discussion of electronic document production, but will be needed to have fruitful discussions about production of data from any database.)

a. For any database that contains information responsive to the Second Request, please specify:

> (1)   the application used (including both the database software and user interface software, along with the versions);
> (2)   the number of users;
> (3)   the size of the database (including both the number of records and bytes); and
> (4)   the number of fields or tables in each database.

b.   Briefly describe the type of business information stored in each database identified in response to 7(a).

c.   Provide copies of the reports run on each database, any data dictionaries, and training materials for users of the databases.