INSPECTION PROCEDURE 88113

CONTROL OF THE ELECTRONIC MANAGEMENT OF DATA

PROGRAM APPLICABILITY: 2630

88113-01 INSPECTION OBJECTIVES

01.01 To establish, by objective evidence, that the management and maintenance of electronic data include a life-cycle management process, from the creation and receipt of records, through active life, storage, and final disposition.

01.02 To determine if electronic data are properly controlled in accordance with the facility's approved quality assurance plan.

88113-02 INSPECTION REQUIREMENTS

02.01 Determine if electronic data are adequately protected, stored, identified, complete and accurate, and secure, and data transfers are properly controlled by verifying the following:

a. Data are suitably protected from damage and destruction during their prescribed lifetime, and are readily retrievable.

b. A description is prepared of how data will be stored, with respect to media, conditions, location, retention time, security, and access.

c. Storage and transfer media are properly identified as to source, physical and logical formats, and relevant date (i.e., date written).

d. Completeness and accuracy of the data input and any subsequent changes are maintained.

e. Data transfers are error-free, or within a defined permissible error rate, to ensure no information is lost in transfer, and the input is recoverable from the output

02.02 Verify that the licensee has established a framework in which record creation and maintenance occur that includes the components noted below:

a. Policies and Procedures.

b. Education and Training.

c. Confidentiality and Integrity.

d. Document Capture.

e. Metadata.

f. File Management.

g. Storage Management.

h. Record Availability.

i. Audit Trail.

j. Retention.

k. Media Renewal or Transfer.

l. Disposal.

88113-03 INSPECTION GUIDANCE

General Guidance.

Selection of areas for evaluation during inspections shall be based on the risk significance of the systems, structures, and components (SSCs), related activities, and past performance. The scope of inspections also should consider the cumulative effect of failures related to low-risk-significant SSCs, regarding their potential effects on overall system performance and reliability.

This inspection procedure typically will be used in conjunction with other inspection procedures that involve data management. While conducting other inspections, if the inspector identifies electronic data use, this inspection procedure may be applied.

Electronic records management requires the records officer to work with the licensee's staff in a life-cycle management process from the creation and receipt of records, through their active life, storage, and to their final disposition. It also requires the participation of every staff member, the cooperation of technology support staff, and the approval of top management.

Before a licensee can begin the process of managing electronic records, it must have an understanding of what it is being managed. This means knowing the difference between documents and records.

Documents are formatted information that can be accessed and used by a person. They have a beginning and an end and may be represented through alphanumeric text, vector data, a digital map, spreadsheets and databases, moving images, or audio data. Regardless of format, documents serve the purpose of conveying information.

Records are documents that have been set aside as evidence and protected from alteration or change. The critical factor is how "set aside" is defined. In paper, "being set aside" means placing a document into a filing system from which it can be retrieved. With digital technologies, the same result is achieved by transferring an electronic document from an operational environment into a record-keeping system.

Elements of a Record.

Content is the information, in a record, the idea or concept, the facts about an event, a person, an organization or other similar act, that are recorded to document the transaction itself.

Structure refers to the physical and logical attributes of records. Physical attributes of a record include such things as the size and style of type, line spacing, page margins, and agency logo. Logical attributes consist of the logical arrangement of the record. For example, the structure of a memorandum would include: (1) a header (the name of the sender, the date, the subject of the memo, and the recipient of the memo); (2) a body (the actual content in one or more paragraphs); and (3) the authentication (signature).

Context explains the "why" of the record. A single record derives its trustworthiness and usefulness from its association with other records that collectively tell the story of an event or activity. A letter from the regulator, for example, may be filed with the letter of response so that anyone viewing the response in the future can see it in the context of the request. Without the request, the response could be taken out of context and misconstrued.

The first two elements of a record are straightforward and easily captured by a single staff member working on a computer. Capturing context involves more than just each person working alone at a computer; it involves a framework, of administrative policies and work procedures, that ensures the creation of authentic electronic records. The checklist in Section 3.02 discusses the issues that will help the inspector evaluate this process.

Specific Guidance.

03.01 No specific guidance provided.

03.02 Record Creation and Maintenance.

a. Policies and Procedures.

For the licensee to control processes and employee behavior, the inspector should verify that the licensee has developed a how-to manual of policies, regulations, standards, and procedures.

1. Policies supply top-level guidance providing a licensee's statement of intent.

2. Regulations provide interpretations of the law and how the law has impact on licensee processes. Regulations also serve to identify all the requirements affecting the performance of a process.

3. Standards establish codes of behavior with regard to the performance of work.

4. Procedures control each step in a process and ensure compliance with standards.

Information in the operating procedures for a computer system should include, at a minimum:

(a) A description of the methods for scanning or entering data;

(b) A description of how records are revised, updated, or deleted;

(c) Hardware and software manuals, including the name of the software, version numbers and dates of installation, upgrades, replacements, and conversions;

(d) A description of how the records are indexed;

(e) Access policies (log-on controls); and security features (e.g., encryption techniques, secure socket-layer encryption technology);

(f) Data structure and content, including the file layout and data dictionaries;

(g) File naming conventions and hierarchy;

(h) Enhancement algorithms (digital-imaging systems);

(i) Backup procedures for disks, tapes, microfilm, etc.;

(j) Procedures for testing the readability of records;

(k) On-line, off-line, near-line storage procedures;

(l) Security safeguards to prevent tampering and unauthorized access to protected information;

(m) Disposition of the records (including over-writing of backup tapes); and

(n) Approved retention schedules.

If the licensee intends to rely on the electronic record as its official record, it is of the utmost importance that a statement of intent to rely on the electronic record exists. Such a statement would identify the electronic record as the licensee's official record. Official records reflect the information and position that the licensee believes are true and complete, and that it will rely on for conducting its business. The official record, once designated by the licensee, must be subject to rigorous procedures for creation, modification, and destruction under a records-management program. A statement designating the electronic record as the official record must exist as part of the licensee's overall records-management program.

b. Education and Training.

1. Verify that licensee staff members comply with policies and procedures and are aware of the procedures and understand them. Ensure that the licensee's training efforts convey the following:

(a) Policies and procedures;

(b) New/revised processes;

(c) What records staff must keep in order to document the process;

(d) The fact that everyone (not just the information technology office) is responsible for creating authentic records; and

(e) Retention and disposition.

2. Training is a vital element of compliance. It is the primary way in which a licensee communicates what it wants done and how it wants it done. Training is an ongoing effort. It should provide a review of existing policies and procedures for staff and an introduction to new policies and procedures.

c. Confidentiality and Integrity.

1. Confidentiality and integrity refer to protecting records from unauthorized access or change in an active environment. This can be accomplished through access controls, authorizations, encryption of documents, and endorser techniques. To ensure the integrity of licensee records, adequate protection against tampering, alteration, revision, and deletion must be included as part of the electronic system. Such protections must exist throughout the entire life span of the records.

2. It is important to remember that documents can be revised; however, records are never altered. Records should be protected as read-only and never over-written. Revisions must be done only as copies, which then become new records. These controls must also be considered in migration planning, so that records are not altered when they are moved to new technologies.

d. Document Capture.

1. A licensee must capture all three elements—content, structure, and context—to create a record. Content is the most straightforward one to address—ensuring that staff uses the "save command" on a computer is relatively simple. But what happens to the related data sets that make the document a record—the record metadata (discussed below)? All electronic sources of information making a record a record must be captured and maintained, along with the document itself.

2. With imaging systems, it is important to maintain the hardcopy sources, both paper and microforms, until the images can be verified. If the licensee is reformatting a record that has a retention period of more than 15 years, then the original or a microfilm copy should be kept as a backup.

3. Also, consider the issues of quality control and quality assurance. Quality control is the real-time inspection of business processes, to ensure that they are being performed repeatedly and consistently. Quality assurance is the post-process inspection of business processes, to evaluate whether they are working as designed, or if alterations are needed.

e. Metadata.

1. The term metadata literally means data about data or, information about the licensee's records. In addition to indexing information, there are five additional areas of metadata that should be collected and maintained as part of every record. These are:

(a) Accessibility includes information about statutory restrictions that may apply to the record;

(b) Retention and disposition includes information about how long the record is being kept and what is the trigger for destruction (end of year, etc.);

(c) Security information about restrictions on the information as well as information about how the data are encrypted;

(d) Audit trails includes information documenting all actions (for example, revisions) taken on the record; and

(e) Migration includes information on software versions and technology platforms used to create and store the record.

2. These metadata are not necessarily all in electronic format. For example, migration metadata would include the hardware and software documentation manuals created and maintained by the licensee during installation of a system.

f. File Management.

The licensee's file management system is the component that physically takes care of the records during their active and inactive life. A file management system must preserve the integrity of the records through a non-erasable medium or through controls providing the same level of protection. It should manage the entire record, including the associated metadata, audit trails, and histories, through either logical (all records, metadata, audit trails linked as a logical entity) or physical (all records, metadata, audit trails on a single volume of media) means. The file management system must also support the copying, reformatting, or transfer of records across media and through system technology changes. Finally, the system must support the full recovery of records in case of a disaster. This means the system should provide, or have an added component that provides, the ability to duplicate all vital and permanent records, and the software necessary to view the records.

g. Storage Management.

1. The selection and management of the licensee's storage technology — the file format and the storage medium — are very important. When the licensee selects a file format, keep in mind that if the company that owns the patents on that format goes out of business or stops supporting the format, the licensee may be unable to access and view the records. There is no guaranteed way to avoid this, but if the format you adopt is widely used, it is more likely to be supported for years to come. Currently, the leading document file formats are Portable Document Format and Tagged Image File Format (TIFF).

2. A second area where file formats are important is in the management of spreadsheets. Commonly used file formats for converting spreadsheets include Data Interchange Format (DIF) and Comma-Separated Value (CVS) or (comma delimited). However, most vendors provide backward compatibility over several generations of spreadsheet software, so in the short term, it should be possible to convert a spreadsheet in an older version to one in a newer version.

3. A third area of file formats includes those used in the transfer of data and document encapsulation technologies used to make information available on the World-Wide Web. This area is dominated by markup languages such as Standard Generalized Markup Language (SGML), Hypertext Markup Language (HMTL), and Extensible Markup Language (XML). These file formats allow a document to be read and processed by any computer system.

4. The selection of a storage medium (CD-ROM, 3480 Cartridge Tapes, Open Reel Magnetic Tapes, or Digital Versatile Disks (DVDs), etc.) is equally important. Current trends are toward media independence (meaning the storage device will work with computers from many different manufacturers, not just one). The licensee should adopt media that are mainstream, widely-used devices that comply with industry standards – avoid both cutting-edge and obsolete technologies.

h. Record Availability.

A record is available if it can be rendered in a human-readable form, such as a printout or as an image on a computer screen. Records, including associated metadata and audit trails, must be accessible to authorized individuals for the record's entire life span.

i. Audit Trail.

An audit trail documents who, what, when, and why of all actions or events related to documents and records. It is a key component needed to show a responsible chain of custody in case of litigation. An audit trail will document the creator, recipient, content, date of creation, date of revision, date of sending, any and all alterations, and authorizations connected with an individual record.

j. Retention.

The licensee should have an approved retention schedule, that must apply to all electronic records, in addition to the paper records, that is consistent with regulatory requirements. An electronic record is more than just content; the schedule must also consider the retention of the associated metadata and audit trails. The file management system must be capable of notifying the licensee of a retention trigger (such as "10 years from filing date," or "on completion of the case," or "expiration plus 3 years"). Equally important is the ability to place a hold or freeze on all records destruction.

k. Media Renewal, Copy, or Transfer.

1. There are three components involved with the long-term preservation of electronic records: renewal, copy, and transfer.

   (a) Media renewal is the copying of records from one type of medium to the same type. Example: copying records from one 650 megabyte CD to another 650 megabyte CD. There is no change to any of the records.

   (b) Media copying is the copying or reformatting of records from one medium to another. Example: transferring records from a 650 megabyte CD to a 3480-cartridge tape. This may result in a slight change to the record because of the way data are recorded on different media. Therefore, comparing a sampling of the records on the new medium with the same records on the old medium can verify that any changes are insignificant.

   (c) Media transfer or migration is the complete change of the file management system, as you move from one software platform or technology to another. The file format of the record may change as a result of transfer. A bit-by-bit comparison (validation) of each record will be required to preserve the integrity of the records.

2. When copying and transferring records, it is important to remember that not only the content needs to move, but also the metadata, audit trails, and any links must be preserved and moved.

l. Disposal.

1. Disposal is the ability to identify, gain authorization, and completely purge a record from a computer system. Procedures for disposal of records must be consistent with regulatory requirements for record retention and must exist and be implemented consistently. Disposal may be logical or physical, depending on the storage medium for the records.

   (a) Logical disposal is used with non-erasable media. It involves the purging of all metadata, index points, audit trails, and links to the records. Although, the record itself remains in storage, all pointers to it are destroyed, making it inaccessible.

   (b) Physical disposal means removing the record itself from the medium and renders a record non-reconstructable. It must include both the primary storage medium and the backup media.

2. Procedures for the physical destruction of electronic records should be detailed enough to specify the number of overwrites that must occur to a backup tape to ensure the total destruction of the records.

88113-04 INSPECTION RESOURCES

After construction authorization is issued and safety-related construction starts, an initial inspection of procedures and records associated with the management of electronic data should be conducted. Subsequent inspections of procedures and records associated with the management of electronic data should be conducted on an annually. This inspection should consist of one inspector on site for 24-32 hours.

88113-05 REFERENCES

U.S. Code of Federal Regulations, Title 10, Part 70, "Domestic Licensing of Special Nuclear Material."

Duke, Cogema, Stone and Webster, "Mixed-Oxide Fuel Fabrication Facility, MOX Project Quality Assurance Plan (MPQAP)," Docket Number 070-03098, under US Department of Energy Contract DE-AC02-99-CH10888, latest revision accepted by NRC.

Duke, Cogema, Stone and Webster, "Mixed-Oxide Fuel Fabrication Facility Construction Authorization Request," latest revision accepted by NRC.

END

ATTACHMENT 1

Revision History for IP 88113

Commitment Tracking Number	Issue Date	Description of Change	Training Needed	Training Completion Date	Comment Resolution Accession Number
	02/07/07 CN 07-006	IP 88113 is a newly issued procedure. Issued for MOX inspection program to improve effectiveness and efficiency by incorporating and consolidating requirements for inspection and control of electronic management data.	None	N/A	ML070160148