

NRC INSPECTION MANUAL

IRSB

INSPECTION MANUAL CHAPTER 0620

INSPECTION DOCUMENTS AND RECORDS

Effective Date: 07/23/2020

TABLE OF CONTENTS

0620-01	PURPOSE	1
0620-02	DEFINITIONS	1
02.01	Agencywide Documents Access and Management System (ADAMS)	1
02.02	Classified Information	1
02.03	Sensitive, Unclassified Information	1
02.04	Document Types	2
02.05	Docket File	2
02.06	Freedom of Information Act (FOIA)	2
02.07	Handwritten Note	3
02.08	Inspection	3
02.09	Finding	3
02.10	Working Files	3
02.11	Personal Files	4
02.12	Proprietary Information	4
02.13	Records	4
02.14	Regulatory Requirement	5
02.15	Unfettered Inspector Access	5
0620-03	RESPONSIBILITIES	5
03.01	Executive Director for Operations (EDO)	5
03.02	Office Directors and Regional Administrators	5
03.03	Inspector Supervisors	6
03.04	Inspectors	6
03.05	Program Office	6
0620-04	BASIC REQUIREMENTS	7
04.01	Requesting and Obtaining Documents	7
04.02	Controlling Documents and Records	11
04.03	FOIA Requirements	15
04.04	Record Retention and Disposition	16
0620-05	REFERENCES	17
Exhibit 1 – Use of Photos during the Inspection Process or for Informal Training		Exh1-1
Exhibit 2 – Paperwork Reduction Act Statement		Exh2-1
Attachment 1 – Revision History for IMC 0620		Att1-1

0620-01 PURPOSE

01.01 To provide general guidance for requesting, controlling, and dispositioning U.S. Nuclear Regulatory Commission (NRC) inspection documents and records during all phases of the inspection program including construction, fuel cycle facilities, mining facilities, repository facilities, vendor inspections, operating facilities, power reactors, research reactors, license renewal, and materials inspections. This is not intended to replace guidance in relevant agency manual chapters identified in the reference section which serve as the final authority.

0620-02 DEFINITIONS

02.01 Agencywide Documents Access and Management System (ADAMS). A document management and recordkeeping system that maintains the official records of the agency and manages their disposition.

02.02 Classified Information. Records that (1) are specifically authorized, under criteria established by an Executive Order (E.O.) or by statute, to be kept secret in the interest of national defense or foreign policy and (2) are, in fact, properly classified pursuant to such authority. These records normally include information in a document or correspondence that is designated National Security Information, Restricted Data, or Formerly Restricted Data. Such classifications may include, but are not limited to, Top Secret, Secret, and Confidential and are consistent with NRC Management Directive (MD) 12.2, "NRC Classified Information Security Program."

- a. Classified National Security Information. Information that has been determined pursuant to E.O. 13526, "Classified National Security Information," as amended, or any predecessor order or successor order, to require protection against unauthorized disclosure and that is so designated.
- b. Restricted Data. All data concerning the design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but not data declassified or removed from the category pursuant to 42 U.S.C. 2011 et seq., "Atomic Energy Act of 1954," as amended (AEA), Section 142, "Classification and Declassification of Restricted Data."

02.03 Sensitive, Unclassified Information. Safeguards Information (SGI), Safeguards Information-Modified Handling (SGI-M), and Sensitive Unclassified Non-Safeguards Information (SUNSI)/Controlled Unclassified Information (CUI). Refer to <http://drupal.nrc.gov/sunsi> for more information on both SUNSI and CUI, including Personally Identifiable Information (PII) and pre-decisional enforcement information. Continue to use SUNSI guidance until CUI is fully implemented.

- a. Safeguards Information (SGI). Refer to 10 CFR 73, "Physical Protection of Plants and Materials," section 2, "Definitions," and Management Directive (MD) 12.0, "Glossary of Security Terms." An individual's access to SGI requires both a valid "need to know" for the information and an authorization based on an appropriate background check.
- b. Safeguards Information—Modified Handling (SGI-M). Refer to MD 12.0. The SGI-M designation allows certain licensees, vendors, or applicants to have access to certain

Safeguards Information without completing a full background investigation. Within the NRC, SGI-M is handled and stored the same as SGI.

- c. Non-public Information. Refer to <http://drupal.nrc.gov/sunsi>, and 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding," MD 3.4, "Release of Information to the Public," and the "Guidance for Determining the Public Availability of NRC Records," for more information.

02.04 Document Types

- a. Licensee, Vendor, or Applicant Controlled Document. Any document, correspondence, e-mail, or information that is in the licensee's, vendor's, or applicant's document control or file system such as original, inventoried records, or database files (e.g., surveillance tests, operator logs, quality assurance records, cause evaluations, operability evaluations, issue reports, work orders, action requests, procedures, or calculations). These documents are generally required to be retained by the licensee, vendor, or applicant to meet regulatory requirements.

Note: When an inspector creates a copy (e.g., prints, photocopies, or transcribes into written notes) of a licensee, vendor, or applicant controlled document, that document copy would be considered NRC property under NRC possession and control and would therefore be subject to the Freedom of Information Act (FOIA).

- b. NRC Controlled Document. Any document, correspondence, e-mail, or information that requires special handling to restrict access or disclosure. These include documents that contain classified, SGI, and SUNSI/CUI.
- c. Licensee, Vendor, or Applicant Draft Document. A preliminary written document, preliminary sketch, or drawing. A document is considered to be a draft while it is being developed and reviewed. It ceases to be a draft only when it has been approved by responsible management and issued as a final document for implementation (Refer to Inspection Manual Chapter (IMC) 0330, "Guidance for NRC Review of Licensee Draft Documents" for additional guidance).
- d. Inspection Document. Any material that is obtained or developed in preparation for, during, or resulting from the inspection of a licensee, vendor, or applicant such as inspector written notes.

02.05 Docket File. Records (typically stored in ADAMS) or other information related to a specific NRC docket number that provide a complete record of the transactions between the licensee, vendor, or applicant and the NRC, regardless of whether the information has been made publicly available.

02.06 Freedom of Information Act (FOIA). Prescribes the procedures for making agency records available and copying when a member of the public requests them (Refer to MD 3.1, "Freedom of Information Act").

Documents that are in the possession and control of NRC staff at the time a FOIA request is received are considered agency records that must be released under the FOIA unless it is determined that one or more exemptions apply to justify withholding the document, or any portions of the document.

- a. Possession. The agency's physical custody of records
- b. Control. The agency's legal authority for disposition of records in the context of FOIA

Documents, including copies of licensee, vendor, or applicant documents are considered to be in the possession and control of the NRC when they are removed from licensee, vendor, or applicant-controlled space or property, and taken into NRC custody, such as when copies or digital media containing licensee documents are taken into the resident inspector's office or off site by an inspector. However, such documents reviewed electronically on a licensee, vendor, or applicant-controlled network or web site, if not downloaded to an NRC controlled network or printed, are not considered to be in the possession and control of the inspector, unless the licensee, vendor, or applicant has either relinquished control over the document or given NRC authority to use the document as it sees fit. Also, whenever NRC personnel have relied on a document in making a decision or taking action on behalf of the agency, that document is part of the official agency record.

02.07 Handwritten Note. An informal method of communicating information to individual members of the licensee, vendor, or applicant staff during the performance of an inspection (while onsite). Examples include leaving a note on a licensee, vendor, or applicant staff member's desk indicating the inspector had stopped by, or writing down a procedure (e.g., drawing, record) number for a licensee, vendor, or applicant document control clerk to retrieve.

02.08 Inspection. The examination, review, or assessment of any program or activity of a licensee, vendor, or applicant to determine the effectiveness of the program or activity, to ensure that the health and safety of the public and plant or facility personnel are adequately protected, to ensure that the facility is operated safely, and to determine compliance with any established standards, applicable rule, order, regulation, or license condition pursuant to the AEA, the National Environmental Policy Act or other statutory requirement.

02.09 Finding. Refer to IMC 0610, "Nuclear Material Safety and Safeguards Inspection Reports", IMC 0611, "Power Reactor Inspection Reports", IMC 0613, "Power Reactor Construction Inspection Reports", IMC 0614, "Documenting 10 CFR 52 Construction Audit Activities," IMC 0615, "Research and Test Reactor Inspection Reports", IMC 0616, "Fuel Cycle Safety and Safeguards Inspection Reports", and IMC 0617, "Vendor and Quality Assurance Implementation Inspection Reports" for the appropriate definition and context.

02.10 Working Files. (Refer to 36 CFR 1222, "Creation and Maintenance of Federal Records").

Working files, such as preliminary drafts and rough notes, and other similar materials, are generally temporary records that are maintained to ensure adequate and proper documentation until used to create a longer-term record, or superseded by development of another record, or no longer needed, such as to preserve a complete understanding or explanation of an agency action or decision. Examples are inspector written notes, inspector written notes taken on copies of licensee, vendor, or applicant documents, calculations, or drafts assembled or created and used to prepare or analyze other documents such as an inspection report that were obtained in accordance with established inspection practices. Note that most inspection related

working file records are short lived and do not ultimately go into ADAMS (Refer to Section 04.04a for additional guidance).

02.11 Personal Files. Personal files (also called personal papers) are documentary materials belonging to an individual that are not used to conduct agency business and are not needed to properly document agency actions or decisions. Examples include documents such as personal correspondence related to private business, or written notes about agency business that someone makes solely for that person's own use, such as memory refreshers. Personal files are excluded from the definition of Federal records and are not covered by agency records retention schedules.

Personal files should be maintained separately from agency records. Information about private matters and agency business should not be mixed with official business. If information about private matters and agency business appears in a single document, the personal information may be deleted or redacted, and the redacted version treated as a Federal record. The use of a label such as "personal" does not control the status of documentary materials in a Federal agency.

Although personal files are typically not considered agency records subject to a FOIA request, if an employee has responsive records that he or she believes to be personal records, these records are reviewed by the employee using NRC Form 510, "Personal Record Checklist," to determine if the records are personal or agency records. If the employee determines that the records are personal, the completed Form 510 and the personal records are provided to the FOIA Privacy Act staff. Alternatively, the completed Form 510 and personal records may be retained by the office's FOIA coordinator. The FOIA staff will inform the requester in writing of this determination. The personal records must be maintained for 6 years from the date of the NRC's final response to the requester either by the employee, the office FOIA coordinator, or the FOIA staff. For detailed information on FOIA procedures and definitions see MD 3.1.

02.12 Proprietary Information. Records that (1) contain trade secrets and commercial or financial information, obtained from a person or entity as privileged or confidential, the disclosure of which would result in substantial harm to the competitive position of the owner, as supported by an accompanying affidavit signed and notarized by the owner of the information, in accordance with 10 CFR 2.390, (2) contain voluntarily provided information that the submitter would not normally release to the public, or (3) the release of which would harm the Government's ability to obtain information in the future. Refer to <http://drupal.nrc.gov/sunsi> for more information.

02.13 Records:

- a. **Disposition.** Those actions taken regarding records no longer needed for the conduct of the regular current business of the agency. (36 CFR 1220.18, "Inspection of Records")
- b. **Official Records.** All books, papers, maps, photographs, and machine-readable documentary materials regardless of form or physical characteristics created or received by any agency of the United States Government under Federal law or in connection with the transaction of public business and that are preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data contained in these materials (see 44 U.S.C. 3301, "Definition of Records" also 36 CFR 1220.18).

Records created (e.g., copying or printing licensee documents) by the NRC inspector, whether through printing, copying, or reproduction by any means (e.g., inspector written notes), are considered records in the possession and under the control of the NRC.

- c. Privacy Act Records. Any item, collection, or grouping of information about an individual that is maintained by the NRC in a Privacy Act system of records, including but not limited to the individual's education, financial transactions, medical history, employment history, or criminal history, that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph and is retrieved by the individual's identifier. (See MD 3.2, "Privacy Act")
- d. Retention Period. The length of time that records must be kept. (Refer to 36 CFR 1220.18 and, NUREG 0910 "[Comprehensive Records Disposition Schedule](#)")

02.14 Regulatory Requirement. A legally binding obligation such as a statute, regulation, license condition, technical specification, or order.

02.15 Unfettered Inspector Access. Access equivalent to access provided regular plant or facility employees, following proper identification and compliance with applicable access control measures for security, radiological protection and personal safety (See 10 CFR 50.70, 10 CFR 70.55, and 10 CFR 30.52, all titled "Inspections"). Typically, regular plant or facility employees can copy, print, download, or email licensee, vendor, or applicant documents with few restrictions and review such documents. Unfettered access applies only to regulated activities. Refer to Section 04.01b.

0620-03 RESPONSIBILITIES

03.01 Executive Director for Operations (EDO). Approves the release of all inspection documents that have not been officially issued unless specifically authorized under Office Instructions or Management Directives, or any information contained therein, except in cases where release authority for significant safety or safeguards issues has been granted to the office directors or regional administrators.

03.02 Office Directors and Regional Administrators

- a. Establish internal controls to ensure that information collections comply with agency policies and procedures.
- b. Implement existing policies, guidance, and regulatory requirements for the acquisition, control, and disposition of documentation used in preparing for inspections, gained during the conduct of inspections, and resulting from inspections.
- c. Obtain EDO approval before releasing a draft inspection document not specifically authorized by Office Instructions or Management Directives and before discussing the document in a way that is contrary to established NRC policies, procedures, and

regulatory requirements for such occasions as exit meetings and inspector discussions with licensees, vendors, or applicants during inspections.

- d. Notify the EDO immediately if substantive documents (i.e., allegations, investigations, safeguards, proprietary information, or personal identifiable information) are inadvertently released or discussed.
- e. Take required corrective action when inspection documents are released contrary to NRC policies, procedures, regulations, and legal requirements.
- f. Ensure that subordinate managers and staff are cognizant of, and adhere to, the policies and guidance in this IMC.

03.03 Inspector Supervisors

- a. Ensure that their staff is cognizant of, adheres to, and implements the policies and guidance contained in this IMC.
- b. In accordance with this IMC and established policies, procedures, and regulatory requirements, provide for reviews, approvals, or denials of all inspection documentation before release to a licensee, vendor, applicant, ADAMS, or in response to a FOIA request.
- c. As appropriate, immediately inform the respective division, staff, or project director, and the Office of the Chief Information Officer (OCIO) Privacy Officer, when draft inspection documents (i.e., pre-decisional) or substantive documents (i.e., allegations, investigations, safeguards, proprietary information, or personal identifiable information) are inadvertently released to a licensee, vendor, applicant, or the public, contrary to NRC policies, procedures and regulatory requirements, and report the facts concerning the release. As stated on our internal webpage (<http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures>), "Whenever SUNSI is inadvertently released or disclosed by the NRC or its contractors, the office director must promptly inform the Executive Director for Operations (EDO) and the Office of the Inspector General (OIG) in accordance with MD 3.4, "Release of Information to the Public." Refer to MD 3.4 for more information, as well as our internal webpage regarding SUNSI information and spills.
- d. Review and approve docketed notification of inspection and request for information correspondence letters and ensure that information requests are compliant with the Paperwork Reduction Act (PRA).

03.04 Inspectors Follow regulatory requirements, policies, and guidance for the acquisition, control, and disposition of inspection documentation.

03.05 Program Office. Interprets and provides guidance on this IMC with assistance from the Office of Enforcement (OE), Office of General Council (OGC), and OCIO.

0620-04 BASIC REQUIREMENTS

04.01 Requesting and Obtaining Documents

a. Requesting Documents for Inspection Preparation.

1. Requests for documents or information needed either to prepare for an inspection or during an inspection are to be reasonable and should not unnecessarily burden the licensee, vendor, or applicant.
2. Inspectors should not normally request documents that already exist as NRC official records in ADAMS.
3. Inspectors should not normally request draft licensee, vendor, or applicant documents or analyses that do not exist in final, approved form in the licensee's, vendor's, or applicant's document control system. However, on occasion inspectors will need to request and review draft information to verify the adequacy of taken or planned corrective actions as they related to immediate safety concerns or issues, such as compensatory measures taken to address equipment operability for an example. The licensee, vendor, or applicant may choose to provide draft information to the Senior Reactor Analyst (SRA) to support timely and accurate significance determinations or risk assessments (See IMC 0330 for additional details). Inspectors should not act as a consultant with licensees during the course of reviewing draft documents.
4. Inspectors should not request that a licensee, vendor, or applicant generate documents such as analyses, position papers, or calculations, that are not needed to meet a regulatory requirement or demonstrate compliance. Requests to generate non-existent analyses, position papers, or calculations related to regulatory requirements or compliance issues can be addressed using 10 CFR 50.54, "Conditions of Licenses," section (f) as appropriate. Inspectors can request from the licensee, vendor, or applicant specific records in the licensee's, vendor's, or applicant's document control system such as lists of modifications or corrective action program documents sorted by date, subject, status, or another attribute.
5. For team inspections, the lead inspector or team leader should prepare a list of documents that are needed for the inspection or that the inspector would like to have available upon arrival at the site. One accepted practice would be for the lead inspector or team leader to e-mail the notification of inspection and request for information to the licensee, vendor, or applicant far enough in advance to allow for adequate preparations. However, if desired, a letter on the docket can be drafted. The purpose of this is to provide advance notification and avoid placing unnecessary burden on the licensee, vendor, or applicant. Inspectors should communicate lengthy requests for documents to the licensee, vendor, or applicant at least 30 days before the documents are needed when inspection lead time permits. The licensee should be made aware that the documents received through this process may become part of the working file or inspection record which would be subject to the FOIA.

Resident and senior resident inspectors should periodically communicate to appropriate licensee staff the types of documents they will be routinely inspecting and which may be routinely be under NRC possession and control and subject to the FOIA.

6. Corresponding with the licensee, vendor, or applicant via e-mail or phone is appropriate to request additional documents.
7. Documents that contain classified information (i.e. National Security Information and Restricted Data) may not be transmitted via e-mail. SGI may not be e-mailed over an unprotected network unless the files are encrypted on an SGI system using a Federal Information Processing (FIPS) Standard Publication 140-02, "Security Requirements for Cryptographic Modules," compliant version of Pretty Good Protection (PGP) software, then transferred via diskette (in encrypted form) to the local area network (LAN) for e-mail transmission. (Refer to MD 12.2, MD 12.4, "NRC Telecommunications Systems Security Program", and MD 12.7 "NRC Safeguards Information Security Program" for the current policy). SGI and Confidential may be mailed, if properly packaged (mailing of classified information isn't limited to SGI and Confidential). The approved NRC classified mailing address shall be used for classified information. SGI and Confidential data can also be transferred using a secure fax machine with appropriate controls established in agency guidance. SUNSI/CUI encompasses a wide variety of categories (e.g., personal privacy, allegations, pre-decisional, proprietary etc.) handled according to the requirements found on the SUNSI/CUI Web site at <http://drupal.nrc.gov/sunsi>
8. E-mail may also be used for exchanges of general information on administrative activities such as schedules, meeting preparations, and travel plans. Administrative e-mails should not be placed in ADAMS.
9. Some inspections or site visits may require requests for the same information from each of a selected sample of licensees, vendors, or applicants. Under the PRA, if the same information is requested from 10 or more licensees, vendors, or applicants during a 1-year period, a review should be conducted to approve the information collection. Refer to MD 3.54, "NRC Collections of Information and Reports Management," and 5 CFR 1320.3, "Definitions," section (c)(4) for additional information.
10. Letters or e-mails requesting inspection information from the licensee, vendor, or applicant should include a Paper Work Reduction Act Statement which includes a valid OMB control number. Refer to Exhibit 2 for a sample Paper Work Reduction Act Statement and refer to the appropriate section of the CFR to find the applicable OMB control number for your activity (e.g., 10 CFR 30.8, 10 CFR 50.8, 10 CFR 70.8, all titled, "Information collection requirements: OMB Approval,"). To ensure compliance with the PRA, the author will need to verify the accuracy of their PRA statement by contacting the Information Collection Team in OCIO.

b. Obtaining Documents.

The licensee, vendor, or applicant is obligated to provide unfettered access to all licensee documents related to regulated activities and the NRC has the authority to inspect and create inspection records to effectuate the purposes of the AEA, as amended. (Refer to 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," sections (e)(2), and (q), and 10 CFR 73.70, "Records," for further information.)

Inspectors should become familiar with and observe the established licensee, vendor, or applicant document control practices applied to regular plant employees. Inspectors should also openly communicate with the licensee about ongoing inspection activities and should be sensitive to protecting sensitive licensee information such as, personal privacy information or proprietary information from improper disclosure. If not done when the documents were obtained, inspectors should inform the licensee when copies of licensee, vendor, or applicant documents will be removed from the site unless it is believed that informing the licensee, vendor, or applicant would compromise the identity of an alleged or other type of investigation, in which case regional management should be consulted prior to removal. Generally, the licensee, vendor, or applicant should be afforded the opportunity to identify any material it considers sensitive under 10 CFR 2.390, such as, personal privacy information, or proprietary information, to request withholding from public disclosure prior to site removal.

Licensee, vendor, or applicant objections over the NRC's handling of documents should be promptly shared with management. Inspectors should also inform management when they have indications that a licensee, vendor, or applicant could be impeding or interfering with inspections or could be fettering inspector access to determine if a violation of 10 CFR 30.52, 10 CFR 50.70, and/or 10 CFR 70.55 exists or if actions should be taken under Article 235 of the AEA.

Acceptable practices for obtaining licensee, vendor, or applicant documents include but are not limited to the following:

1. Requesting the licensee, vendor, or applicant to send the documents to the regional office addressed to the individual inspector assuming the request does not place unnecessary burden on the licensee, vendor, or applicant.
2. Requesting that the documents be sent electronically to the team leader or lead inspector.
3. Sending a designated inspector to the site to obtain the needed documents from the licensee, vendor, or applicant.
4. Requesting the resident inspector's office staff to retrieve the needed documents from the licensee, vendor, or applicant.
5. Using the licensee's, vendor's, or applicant's computer in accordance with the approved NRC memorandum of understanding between both parties.
6. Using the licensee's, vendor's, or applicant's copy machine to make copies of materials relevant to the inspection.

7. Using the licensee's, vendor's, or applicant's intranet or equivalent to view or download files that the licensee, vendor, or applicant has uploaded. The inspector should inform the licensee that files downloaded by NRC staff will be in the agency's possession and control and as such may be subject to FOIA requests.
8. The use of BOX Enterprise File Synchronization Sharing (EFSS). Staff have the responsibility to protect sensitive NRC information, as directed in non-public Yellow Announcement (YA) 20-044, "Use of External File Share Services," and MD 12.5, "NRC Cybersecurity Program." The use of BOX Enterprise File Synchronization Sharing (EFSS) has been approved as the agency's file sharing solution for Sensitive Unclassified Non-Safeguards Information (SUNSI). No other solution shall be used for NRC-initiated file sharing of business information.

In cases where an external entity such as a licensee or another agency initiates an invitation, file sharing services other than BOX-EFSS may be used to collaborate on non-NRC information. When receiving an invitation from an external entity, register an account using your NRC e-mail address. No NRC SUNSI information should be exchanged using these file share solutions.

While the scope of MD 12.5 does not include the handling of personal Personally Identifiable Information, staff should review and consider the privacy capabilities of file sharing solutions to ensure adequate protection of their information. When handling personal data using an NRC device, staff should refer to and follow guidance in MD 2.7, "Personal Use of Information Technology."

Summary Table

<u>NRC Work-Related</u>				
<u>Activity</u>	<u>Solution</u>	<u>Audience</u>	<u>E-mail Account</u>	<u>Information Type</u>
Sharing NRC data	BOX-EFSS	Licensees, Contractors, or NRC staff	NRC	SUNSI
Invited to share by external entity	Licensed solution by external entity	Licensees, Contractors, or NRC staff	NRC	Non-SUNSI
<u>Non-NRC Work-Related</u>				
Sharing personal data	Refer to MD 2.7, Personal Use of Information Technology	Self or someone else	Personal	Personal data

Note: If a licensee, vendor, or applicant asserts that any of the documents or document excerpts to be retained by an inspector as an NRC official record contain proprietary or company classified information, the NRC should advise the licensee, vendor, or applicant to submit an application for withholding pursuant to 10 CFR 2.390 section (b)(1) with the required affidavit before any of the documents are placed in ADAMS in

accordance with Section 04.04a. The licensee, vendor, or applicant must provide the affidavit to the lead inspector or team leader at the exit meeting or within 10 working days after the exit meeting.

Issuance of a suspension order may be appropriate when a licensee is not reasonably cooperating with legitimate NRC requests for documents. It would not typically be expected that the NRC would need to resort to a subpoena for licensee documents that are required to support regulatory oversight.

04.02 Controlling Documents and Records

- a. **Use of Cameras and Recording Devices.** Inspectors and inspection team leaders should ensure that the licensee, vendor, or applicant is made aware that inspectors may be taking photographs or recordings during the course of their normal inspection activities. Inspectors are expected to openly communicate and observe all established licensee, vendor, or applicant procedures for photography or recording, including the prohibition of flash photography in areas of sensitive equipment. The licensee, vendor, or applicant may not impede or interfere with inspections by limiting the use of NRC cameras or recording devices (See Article 235 of the AEA). Sensitive photographs or recordings requiring protection under 10 CFR 2.390 should be appropriately marked. Photographs or recordings should be properly classified by inspectors prior to e-mailing or transmitting off site. Refer to Exhibit 1 for further guidance on the use of photographs during the inspection process.
- b. **Written Notes and Electronic Correspondence**
 1. Inspectors and SRAs should be aware that written notes or e-mails provided to a member of the licensee's, vendor's, or applicant's staff or received by NRC staff in the transaction of Government business may need to be preserved as records in the working file to either be ultimately retained in ADAMS or disposed of in accordance with Section 04.04a, "Record Retention and Disposition." Inspectors should be aware that working files and licensee, vendor, or applicant responses may be publicly released in response to a FOIA request.
 2. Handwritten notes should not be used to request a response to a specific question from licensee, vendor, or applicant but may be used to request a reasonable number of specific documents during the course of an inspection. Reviewed documents should be listed in the inspection report in accordance with inspection report writing requirements. It is also acceptable for an inspector to leave a brief handwritten note on the desk or at the work station of a licensee, vendor, or applicant employee indicating that the inspector had stopped by while the employee was out of the office. This handwritten note should be limited to the inspector's name, the date and time of the visit, a brief description of the topic to be discussed, and information related to how or when the inspector would like to be contacted in the future.
- c. **Inspector Written Notes (Working Files).** Inspectors written notes are working files as defined in Section 02.10 and are generally discarded after the inspection report is finalized, since the information deemed relevant to any inspection issue has been captured in the final inspection report. Inspector's written notes shall not be shared with

the licensee. Written notes that discuss preliminary results/findings of an inspection should be reviewed in accordance with MD 12.

- d. Team Meetings, Licensee, Vendor, or Applicant Debrief, and Exit Meetings. The team leader normally makes an integrated list of the significant inspection observations identified at team meetings; the observations are considered inspector's written notes. As a courtesy, the team leader or lead inspector discusses them daily with licensee, vendor, or applicant management to ensure effective and efficient communications at the exit meeting. It is acceptable to use a dry erase white board, as well as a Power Point presentation, during the licensee, vendor, or applicant debrief as a discussion aid. Power Point presentations, used in an exit debrief to provide a proper understanding of agency decisions and actions, should be placed into ADAMS as a non-public official agency record (Refer to MD 3.53). However, a written list of preliminary inspection findings is not to be given to licensee, vendor, or applicant management. If it is given to the licensee, vendor, or applicant, it is to be declared as a record and placed in ADAMS and may be requested under FOIA.
- e. Storage and Disposal of Inspector Written Notes and Materials
 - 1. Working files and records should be organized, for ease of incorporation into longer-term records. Working files may be discarded once superseded or when no longer needed.
 - 2. While onsite, inspectors shall ensure that draft material or written notes developed at licensee, vendor, or applicant facilities are appropriately disposed of when no longer needed. This precaution is to ensure that the licensee does not inadvertently review pre-decisional or draft information.
 - 3. Before using licensee, vendor, or applicant facilities for the disposal of an inspector's documents or written notes, the inspector should determine whether the information, if made available to the licensee, vendor, or applicant, would interfere with the NRC's ability to effectively regulate. If so, the disposal of these materials shall be done at an NRC facility, ex. Resident or regional office. (An example would be notes from the inspection that contain information which may lead to a specific inspection decision being shared with a licensee prior to inspection results that are published in an inspection report.)
 - 4. Inspectors shall continually assess the need to maintain copies of licensee, vendor, or applicant documents and working file documents. Inspectors should limit documents to only those which provide information of significance for the NRC's oversight or will be retained as NRC official records. This policy reduces the administrative burdens associated with retaining unnecessary records.
 - 5. Inspection teams should arrange with the licensee, vendor, or applicant to store inspection-related copies of licensee, vendor, or applicant documents not actively being reviewed outside the resident inspector's office, especially when the team is off site. Inspectors should not lock licensee, vendor, or applicant documents in an NRC controlled locker outside of the residence inspector's office.

f. Licensee, Vendor, or Applicant Controlled Information and Space

1. Inspectors should inform licensee, vendor, or applicant management before the inspection that they might request documents from the licensee's, vendor's, or applicant's document control staff.
2. When the licensee, vendor, or applicant uses a form to request controlled documents from its storage facility or document control clerks, the inspector may fill out this form following the licensee's, vendor's, or applicant's procedures.
3. Inspectors may review licensee, vendor, or applicant-controlled documents and records at any time during the inspection on licensee, vendor, or applicant owned property. This also includes any licensee-controlled documents maintained by the licensee in the resident inspector's office. Inspectors should not remove controlled documents from the licensee's, vendor's, or applicant's property or resident inspector's office, or dispose of it without informing the licensee. Confidential commercial information (e.g., third party accreditation reports) should be reviewed on licensee-owned property outside of the Resident Inspector's Office to the extent possible and generally should not be reproduced by NRC inspectors unless required to support regulatory oversight.
4. Office space provided on site and outside of the residence inspector's office for inspections or record reviews is not considered NRC office space, even if the licensee provides a key to the NRC. In this space, licensee, vendor, or applicant documents reviewed by inspectors are considered to be in the possession of licensee unless added to the NRC working file by the inspector. Inspectors should be aware that if they take written notes on licensee, vendor, or applicant documents, the documents become part of the working file record which shall ultimately be disposed of or retained in accordance with Section 04.04a. Licensee, vendor, or applicant documents reproduced by the NRC or given to the NRC by licensee staff may be added to the NRC working file by the inspector. While in the NRC's possession, these documents are subject to FOIA. *NRC staff should take appropriate precautions to protect information in this type of space.*

g. Licensee, Vendor, or Applicant Forms and Written Documentation

1. Some licensees, vendors, or applicants supply forms for inspectors to use during inspections, for written questions or to request information and documents that are needed to continue the inspection. Inspectors shall only use licensee, vendor, or applicant-generated forms to request records and documents. All other information (e.g., questions) should be requested verbally. Some licensees, vendors, or applicants may document and track an inspector's questions and then generate written interim and final answers to these questions. These written licensee, vendor, or applicant generated responses can be reviewed by the inspector during the on-site inspection.
2. Written answers by licensee, vendor, or applicant personnel on a licensee, vendor, or applicant form, in response to verbal questions by an inspector, which the inspector retains after leaving the site as the basis of an inspection finding, are also NRC official records subject to public disclosure. The inspector shall

notify the licensee, vendor, or applicant that the retained form will be considered an NRC official record subject to potential public disclosure and provide the licensee, vendor, or applicant the opportunity to request that the information be withheld pursuant to the requirements of 10 CFR 2.390 section (b)(1).

3. Written answers provided in response to inspector questions are considered working files and managed according to the instructions in Section 04.04a. Written answers provided on licensee, vendor, or applicant forms that do not provide the basis for a substantiated inspection conclusion (i.e., finding) generally are not ultimately retained by the NRC as official records in ADAMS. The licensee, vendor, or applicant may decide the disposition of licensee, vendor, or applicant forms not retained by the inspector that do not otherwise need to be maintained under regulatory requirement.

h. Release of Information before Inspection Report Issuance

1. Discussions with licensees, vendors, or applicants related to information contained in the inspection report should be limited to the observations made by the inspector during the inspection and the inspector's preliminary assessment of the observation. It is helpful to verbally share information such as influential assumptions, exposure time information, common cause modelling assumptions, etc., but it is essential to maintain our independence as well.
2. Consistent with NRC policies, procedures and regulatory requirements, no portion of any inspection report or draft inspection documents shall be shown to or given to licensees, vendors, or applicants, or to any other group or person external to the NRC before formal issuance of the inspection report, without the explicit permission of the EDO (Refer to MD 3.4, "Release of Information to the Public"). This includes, but is not limited to, documentation containing cut-sets in support of detailed risk evaluations performed in accordance with IMC 0609, "Significance Determination Process."
3. If inspection documentation is inadvertently or improperly released, the affected Office Director or Regional Administrator shall inform the EDO in writing as to the facts concerning the release within 30 days or sooner if reporting to U.S. Computer Emergency Readiness Team (CERT) in response to a data spill. The responsible office or region should take corrective action to retrieve the documentation and prevent recurrence of such a release. Refer to MD 3.4 for more information.
4. If inspection documents or inspection-generated information are inadvertently left unattended for a period of time in a non-NRC controlled area or public space, it should be determined whether the subject matter was reviewed in detail by third parties or if a substantive release of information occurred. If release of information is evident, the division director should be notified for further discussion and any security related aspects of the release should be address in accordance with MD 12.2.
5. If e-mail is being used to convey pre-decisional inspection information, inspectors shall be mindful of the type of information they put in emails, as well as the names listed in the "To," "cc," and "bcc" fields. Emails have the potential to be

misconstrued or taken out of context, if inadvertently released to the public or released through a FOIA request. Use of e-mail groups, which only contain NRC staff members, is encouraged to reduce the risk of MS Outlook sending e-mail to unintended recipients by using the auto-complete function.

6. Existing technologies, such as shared internal drives, SharePoint, or Skype, are alternate ways to communicate sensitive information versus email. These methods can ensure that only those within the NRC have access to the information if used properly. A concerted effort should be made by staff and management to learn how to utilize the existing tools available and find ways to integrate use of these tools into current practices. Staff using these types of technologies shall be discouraged from extracting files from such sites and attaching them to emails, a practice that negates the security controls provided by these technologies. Rather, staff wishing to reference a document using one of these options should provide a link to the site in their NRC staff group email address.
7. Significant safety or security-related information shall be promptly and clearly communicated to responsible licensee, vendor, or applicant management to obtain prompt evaluation and corrective action. There are few circumstances where this information cannot be relayed orally. Therefore, no draft inspection documents shall be given to the licensee, vendor, or applicant unless the issue is so time-critical that oral communication will not suffice to prevent or mitigate an emergency or significant safety or safeguards event (e.g., accidental criticality, core damage). Under these circumstances prior EDO approval would not be required.
- i. Additional Controls and Marking Requirements. Sensitive unclassified information shall be marked and controlled in accordance with MD 12.2, 12.7, and the SUNSI/CUI Handling Requirements (<http://drupal.nrc.gov/sunsi>).

04.03 FOIA Requirements

- a. Records that are in the possession and control of the NRC are subject to the FOIA. Examples of such records include but are not limited to, the following:
 1. Memoranda, facsimile transmissions (faxes), voicemails, and electronic files, such as Word files, e-mail, and databases.
 2. Licensee, vendor, or applicant documents, including but not limited to photographs, diagrams, and video recordings, which may be controlled, uncontrolled, or in draft form which are in the possession and under the control of an NRC inspector such as those files or records maintained in the working file.
 3. NRC-originated photographs, videos, or sound recordings that are in the possession of the NRC staff.
 4. Documented or transcribed conversations.
 5. Inspector written notes that have been shared with others or commingled with NRC official records.

6. Background material in the possession and control of the NRC staff.
7. Preliminary inspection findings.
- b. Documents may be withheld in part or in their entirety for information that falls within one or more of the FOIA exemptions defined in 10 CFR Part 9, "Public Records," (See MD 3.1 for more detailed explanations of FOIA exemptions).

Note: A copy of all records that are within the scope of the FOIA request must be provided. Any record to be withheld in part or in its entirety must be bracketed with the appropriate FOIA exemption noted.

04.04 Record Retention and Disposition

- a. **Retaining Records.** All Federal agencies must make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. Inspectors and SRAs are to retain the essential information necessary to document the formulation of inspection and licensing conclusions and inspection-related agency decisions and actions (ex., documents, records, and correspondences including e-mail that provide the basis for an inspection finding, significance determination, or licensing action). If the information would be needed to explain or support the actions of decisions of the NRC the documents should be preserved in the official file. Working file records can be destroyed after they are incorporated into a final product such as an issued inspection report provided that they are not needed to fully document the agency's actions or decisions. Supporting or supplemental inspection documentation related to inspection findings or violations would not normally be maintained after the issuance of the final inspection report or beyond the time period afforded for any licensee appeals. Supporting or supplemental inspection documentation should normally only be referenced in the inspection report when it can be readily retrieved from the licensee document control system or files.
- b. The documents listed below, with the notable exceptions of those including SGI which is typically stored in the SGI LAN Electronic Safe (SLES), pre-decisional enforcement documents, and allegations files are required to be declared as records and placed in ADAMS:
 1. Written correspondence, including e-mails and faxes, to the licensee, vendor, or applicant that were required to substantiate regulatory conclusions (i.e., findings, significance determination, or licensing action).
 2. Team inspection notification and document request letters generated per Section 04.01a.5.
 3. Inspection reports.
 4. Photographs, videos, or recordings that do not contain personal privacy, classified, proprietary, or safeguards information, that were required to

substantiate regulatory conclusions (i.e., findings, significance determination, or licensing action).

5. Documents or excerpts of documents retained by an inspector that were used to substantiate regulatory conclusions (i.e., findings, significance determination, or licensing action).
6. Where approved by the EDO, written lists of significant inspection issues requiring prompt corrective action that have been provided to the licensee, vendor, or applicant. This list should be attached to the inspection report or meeting summary when issued.
7. Any documentary information related to inspection activities that an NRC inspector distributes or presents (e.g., PowerPoint presentation) at a management meeting with the licensee, vendor, or applicant. Such written material must be placed in ADAMS and attached to or referenced in the inspection report or meeting summary.

Note: Documents or portions of documents that meet the requirements of 10 CFR 2.390 section (b), the exceptions to the definition of “agency record” found at and 10 CFR 9.13, “Definitions,” and 10 CFR 9.17, “Agency Records Exempt from Public Disclosure,” generally would not be made publicly available, subject to applicable FOIA law and policy.

- c. Destruction. Documents and records which are not retained and contain sensitive unclassified information must be destroyed in a manner which prevents reconstruction of the information (e.g., shredded). Sensitive unclassified information may also be placed in receptacles designated for classified waste or approved for sensitive unclassified. For further information on document destruction, see the SUNSI/CUI Handling Requirements (<http://drupal.nrc.gov/sunsi>). For information on handling classified information or SGI, See MD 12.2 or MD 12.7.

0620.05 REFERENCES

5 CFR 1320.3, “Definitions”

10 CFR 2.390, “Public Inspection Exemptions, Requests for Withholding”

10 CFR 9, “Public Records” (FOIA’s, Privacy Act Information)”

10 CFR 9.13, “Definitions”

10 CFR 9.17, “Agency Records Exempt from Public Disclosure”

10 CFR 30.8, “Information Collection Requirements: OMB Approval” (Materials)

10 CFR 30.52, “Inspections” (Materials)

10 CFR 50.54, “Conditions of Licenses”

10 CFR 50.70, "Inspections" (Power Reactors)"

10 CFR 50.8, "Information collection requirements: OMB approval" (Power Reactors)"

10 CFR 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"

10 CFR 70.8, "Information collection requirements: OMB approval" (Special Nuclear Material)"

10 CFR 70.55, "Inspections" (Special Nuclear Material)"

10 CFR 73, "Physical Protection of Plants and Materials"

10 CFR 73.2, "Definitions"

10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage"

10 CFR 73.70, "Records"

36 CFR 1220.18, "Inspection of Records"

36 CFR 1222, "Creation and Maintenance of Federal Records"

42 U.S.C. 2011 et Seq., "Atomic Energy Act of 1954"

44 U.S.C. 3301, "Definition of Records"

E.O. 13526, "Classified National Security Information"

FIPS PUB 140-02, "Security Requirements for Cryptographic Modules"

| **MD 2.7, Personal Use of Information Technology"**

MD 3.1, "Freedom of Information Act"

MD 3.2, "Privacy Act"

MD 3.23, "Mail Management"

MD 3.4, "Release of Information to the Public"

MD 3.53, "NRC Records and Document Management Program"

MD 3.54, "NRC Collections of Information and Reports Management"

MD 12, "Security"

MD 12.0, "Glossary of Security Terms"

MD 12.1, "NRC Facility Security Program"

MD 12.2, "NRC Classified Information Security Program"

MD 12.4, "NRC Telecommunications Systems Security Program"

MD 12.5, "NRC Cybersecurity Program,"

MD 12.7, "NRC Safeguards Information Security Program"

IMC 0330, "Guidance for NRC Review of Licensee Draft Documents"

IMC 0609, "Significance Determination Process"

IMC 0610, "Nuclear Material Safety and Safeguards Inspection Reports"

IMC 0611, "Power Reactor Inspection Reports"

IMC 0613, "Power Reactor Construction Inspection Reports"

IMC 0614, "Documenting 10 CFR 52 Construction Audit Activities"

IMC 0615, "Research and Test Reactor Inspection Reports"

IMC 0616, "Fuel Cycle Safety and Safeguards Inspection Reports"

IMC 0617, "Vendor and Quality Assurance Implementation Inspection Reports"

"Guidance for Determining the Public Availability of NRC Records" (non-public)

NRR OI COM-203, "Informal Interfacing and Exchange of Information with Licensees and Applicants" (non-public)

NUREG-0910, "Comprehensive Records Disposition Schedule"

Exhibit 1 – Use of Photos during the Inspection Process or for Informal Training

USE OF PHOTOS DURING THE INSPECTION PROCESS		
QUESTION	ANSWER	SOURCE
1. Should I inform the licensee, vendor, or applicant prior to taking photographs?	<p>The licensee, vendor, or applicant should be made aware that the NRC may be taking photographs during all inspection activities.</p> <p>Requests by the licensee, vendor, or applicant to review photographs for personal privacy, classified, proprietary, or safeguards information should normally be honored.</p> <p>Use common sense in taking photographs as part of your routine inspection activities. Avoid taking photographs of personnel or plant or facility features related to security when irrelevant to the inspection. Follow the licensee's policy on the use of photographic equipment, including the prohibition of flash photography in areas of sensitive equipment.</p>	IMC 0620, "Inspection Documents and Records"
2. What if the licensee, vendor, or applicant objects to taking photographs?	All licensee objections should be considered seriously. If photographs require protection under 10 CFR 2.390, they should be appropriately marked and controlled. Inspectors will often need to use photography to effectively document inspection-related agency decisions and actions. Objections to photography based on actual safety or security concerns should be evaluated, but the licensee, vendor, or applicant should not impede or interfere with NRC inspections by limiting the use of NRC cameras. Inspectors should share any licensee's, vendor's, or applicant's concerns with their regional management when objections are raised.	
3. Can I forward photographs to my management electronically without the licensee's, vendor's, or applicant's review?	Yes, after the photograph is classified and appropriately controlled it can be electronically forwarded to management (Refer to Question 5 for additional guidance). The inspector should consider obtaining the licensee, vendor, or applicant review to ensure an accurate classification when deemed appropriate. Inspection related photographs should be controlled to prevent public disclosure except as allowed by established Government processes (e.g., EDO's permission, inspection report issuance, or FOIA).	IMC 0620, "Inspection Documents and Records"

USE OF PHOTOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	SOURCE
4. Do I need something in writing from the licensee, vendor, or applicant that says it has reviewed the pictures for classified, safeguards, SUNSI/CUI?	No. However, requests by the licensee, vendor, or applicant to review photographs for classified, safeguards, or SUNSI/CUI (personal privacy or proprietary information) information should normally be honored so as to ensure proper classification. Appropriate steps should be taken to protect photographs when sensitive information is discovered.	
5. Is there agency guidance on how to forward photographs that contain classified or sensitive unclassified information?	<p>Yes. Photographs that contain proprietary information or are SUNSI/CUI can be forwarded electronically (via email or fax). Photographs that contain unencrypted classified or SGI cannot be forwarded via email over an unapproved network or unsecured fax (Refer to Section 04.01a7 for additional guidance).</p> <p>Also, all photographs believed to contain classified information, SGI, or SUNSI/CUI must be marked in accordance with applicable requirements. Camera film, digital memory, and the recording media used to take the classified photographs must be appropriately protected and secured when unattended.</p>	<p>MD 12.2, "NRC Classified Information Security Program"</p> <p>MD 12.4, "NRC Telecommunications Systems Security Program" SUNSI/CUI Handling Requirements (http://drupal.nrc.gov/sunsi)</p>

USE OF PHOTOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	SOURCE
6. How do I know when photographs must be retained?	<p>If the photographs are used to substantiate an inspection finding and they do not contain classified or safeguards information, they should be retained and placed into ADAMS. (Refer to Section 04.04a for additional guidance)</p> <p>Examples of photographs used to substantiate an inspection finding include photographs that are relied on to support regulatory decision making. In some cases, the photograph may form part of the basis for the inspection finding.</p>	<p>MD 12.1, "NRC Facility Security Program" IMC 0620 "Inspection Documents and Records"</p> <p>NRC authority under the Atomic Energy Act of 1954</p>
When are photographs required to be destroyed?	<p>If the photographs are not used to substantiate an inspection finding they may be destroyed in accordance with NRC guidance for working files in 04.04a.</p> <p>Examples of photographs not used to support an inspection finding include: (1) those photographs that are used as memory joggers to assist the inspector in finalizing the inspection report and (2) photos forwarded electronically to regional management to clarify or to discuss findings. Photographs of this nature generally are not relied on for regulatory decision making.</p>	
7. What if the licensee, vendor, or applicant requests that a photograph be withheld from public disclosure because it contains personal privacy or proprietary information?	<p>When the licensee, vendor, or applicant seeks to withhold from public disclosure a photograph containing SUNSI/CUI (proprietary or privacy information), the NRC should advise the licensee, vendor, or applicant to submit an application for withholding pursuant to 10 CFR 2.390(b)(1). If the information is proprietary the request must be accompanied by an affidavit.</p> <p>If the photograph is the basis for a finding, it may be edited by the licensee, vendor, or applicant to delete the sensitive information unless that information is necessary to support the finding.</p> <p>REMINDER, See IMC 0620</p>	<p>10 CFR 2.390(b)(1)</p> <p>MD 12.1, "NRC Facility Security Program"</p>

USING PHOTOS FOR INFORMAL TRAINING

QUESTION	ANSWER	SOURCE
8. If photographs are not used to support inspection findings can they be retained for training purposes?	<p>If the photographs do not contain classified, safeguards information, or SUNSI/CUI (personal privacy or proprietary), they may be retained for informal training purposes.</p> <p>If the photographs contain classified, safeguards information, or SUNSI/CUI (personal privacy or proprietary), then they should be destroyed unless such information is absolutely necessary to support formal training objectives.</p>	<p>NRC authority under the Atomic Energy Act of 1954</p> <p>IMC 0620, "Inspection Documents and Records"</p>
9. Do I need the licensee's, vendor's, or applicant's permission to keep these photographs?	<p>You do not need the licensee's, vendor's, or applicant's permission to retain these photographs for training purposes if you believe these photographs would be helpful in carrying out NRC's regulatory responsibilities.</p> <p>Requests by the licensee, vendor, or applicant to review photographs for classified, safeguards, or SUNSI/CUI (personal privacy or proprietary information) information should normally be honored to ensure proper classification.</p>	<p>NRC authority under the Atomic Energy Act of 1954</p>
10. Are training photographs subject to FOIA?	Yes.	MD 3.1, "Freedom of Information Act"
11. How should the photographs be identified?	<p>Photographs that contain proprietary information must be labeled as such in accordance with 10 CFR 2.390(b) and should include the date and name of the facility or facility owner.</p> <p>Photographs should be documented and classified as they are produced.</p>	<p>10 CFR 2.390</p> <p>36 CFR 1237.28(h).</p>

USING PHOTOS FOR INFORMAL TRAINING

QUESTION	ANSWER	SOURCE
12. If the photographs contain classified and safeguards information can they still be used for training purposes?	Yes, but only if absolutely necessary and only if the photographs support an inspection finding (REMINDER, Staff reviewing such photographs must possess the appropriate clearance levels and have a “need to know”). If this is the case, such photographs and or digital cameras that contain classified and safeguards information must be secured and agency guidance followed. Follow guidance in IMC 0620 regarding licensee, vendor, or applicant review of such photographs.	IMC 0620, “Inspection Documents and Records” MD 12.1, “NRC Facility Security Plan” MD 12.2, “NRC Classified Information Security Program”
13. Are photographs used for training purposes required to go in ADAMS?	No, if the photographs are used for informal training (on the job training (OJT) and learning opportunities). Yes, if the photographs are used for formal training (e.g., Technical Training Center). Note: SGI photographs would be stored on the SLES or on another approved storage location for training.	MD 3.53, “NRC Records Management Program”
14. How long should photographs used for informal training (OJT and learning opportunities) be retained?	Photographs should be destroyed when they are no longer needed.	
How long should photographs used for formal training be retained?	Currently, the only formal training is through the Human Resources/Technical Training Division, and retention schedules exist for them. Regional offices typically provide only informal training.	

Exhibit 2 – Example of a Paperwork Reduction Act Statement

“PAPERWORK REDUCTION ACT STATEMENT

This letter contains voluntary (mandatory) information collections that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). The Office of Management and Budget (OMB) approved these information collections (approval number 3150-XXXX). The burden to the public for these information collections is estimated to average X hour(s) per response. Send comments regarding this information collection to the Information Services Branch, Office of the Chief Information Officer, Mail Stop: O-1F13, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-XXXX) Office of Management and Budget, Washington, DC 20503.

Public Protection Notification

The NRC may not conduct nor sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

Note: Refer to the appropriate section of the CFR to find the applicable OMB control number for your activity (e.g., 10 CFR 30.8, 10 CFR 50.8, 10 CFR 70.8)

Note: The example PRA statement above is not appropriate in all cases and cannot be used without the permission of the Agency Clearance Officer.

It is good practice to always check with a member of the OCIO Information Collections Team when referring to specific sections of the CFR to find the applicable OMB control number.

Attachment 1 – Revision History for IMC 0620

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	07/08/96 CN 96-015	Revised to ensure compliance with the National Archive and Records Administration (NARA) regulations relating to the creation and retention of federal agency records.	N/A	
N/A	ML053330558 01/27/06 CN 06-002	Completed 4-year review for commitments. Eliminated the requirement to list all documents reviewed as an attachment to the inspection report and the requirement to place all documents reviewed in ADAMS. Updated and added security documents that contain classified information. Added guidance on the use of e-mail during the inspection process.	N/A	
N/A	ML083540780 05/15/09 CN 09-013	Added amplifying information on written requests for information, updated definitions and references.	N/A	ML083540770
N/A	ML093270149 09/12/11 CN 11-015	Improve guidance on unfettered access, possession, and control. Added policy to inform licensee prior to removing copies of licensee controlled documents from the site and for inspectors to purge unnecessary licensee documents when no longer reasonably needed (FF 0620-1484). Revised the record retention guidance to conform to 36 CFR. Added guidance on information requests including the required Paperwork Reduction Act Statement.	N/A	ML100332132

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML18254A020 01/28/19 CN 19-003	Clarified guidance for marking, handling and transmitting inspection documents/written notes internally and externally to ensure all types of documents are appropriately controlled and handled by inspectors. Updated information regarding FOIA, PRA and Privacy. Revised to address feedback form 0620-2252	N/A	ML18254A021 0620-2252 ML18255A152
N/A	ML20196L754 07/23/20 CN 20-034	Revised to add guidance on electronic file sharing, as noted in Yellow Announcement (YA) 20-0044, and MD 12.5, "NRC Cybersecurity Program"	N/A	N/A