

NRC INSPECTION MANUAL

IRIB

INSPECTION MANUAL CHAPTER 0620

INSPECTION DOCUMENTS AND RECORDS

Effective Date: 02/20/2026

CONTENTS

0620-01 PURPOSE.....2

0620-02 DEFINITIONS.....2

 02.01 Agencywide Documents Access and Management System (ADAMS).....2

 02.02 Classified Information2

 02.03 Sensitive, Unclassified Information2

 02.04 Document Types.....3

 02.05 Docket File4

 02.06 Freedom of Information Act (FOIA).....4

 02.07 Handwritten Note5

 02.08 Inspection.....5

 02.09 Finding5

 02.10 Working Files5

 02.11 Personal Files6

 02.12 Proprietary Information6

 02.13 Records.....7

 02.14 Regulatory Requirement7

 02.15 Unfettered Inspector Access.....7

0620-03 RESPONSIBILITIES8

 03.01 Executive Director for Operations (EDO).....8

 03.02 Office Directors and Regional Administrators8

 03.03 Inspector Supervisors8

 03.04 Inspectors8

0620-04 BASIC REQUIREMENTS.....8

 04.01 Requesting, Obtaining, Reviewing, & Disposing of Inspection-Related Information...9

 04.02 Documents and Records During Inspection Activities13

 04.03 FOIA Requirements18

 04.04 Record Retention and Disposition19

0620-05 REFERENCES.....20

Exhibit 1: Use of Photographs or Videos During Inspection or for Informal Training Ex1-1

Exhibit 2: Example of a Paperwork Reduction Act Statement Ex2-1

Attachment 1: Revision History for IMC 0620 Att1-1

0620-01 PURPOSE

01.01 This Inspection Manual Chapter (IMC) provides general guidance for requesting, creating, controlling, and dispositioning documents and records **throughout** all phases of the U.S. Nuclear Regulatory Commission (NRC) inspection programs. It does not replace guidance in relevant agency **documents** identified in the reference section which serve as the final authority.

0620-02 DEFINITIONS

02.01 Agencywide Documents Access and Management System (ADAMS)

ADAMS is a document management and recordkeeping system that maintains the official records of the agency and manages their disposition. **For a listing of records that are not added to ADAMS, see “Guidance for Determining the Public Availability of NRC Records,” (ML072770468) updated in July 2024; it provides guidance to determine which documents are generally made publicly available. Also see NRC Management Directive (MD) 3.4, “Release of Information to the Public,” to determine ADAMS profiling for public or non-public documents.**

02.02 Classified Information

Information that has been determined, pursuant to an Executive Order or by statute, to require protection against unauthorized disclosure and is classified pursuant to such authority. Classified information includes designated National Security Information, Restricted Data, and Formerly Restricted Data. Such classifications may include, but are not limited to, Top Secret, Secret, and Confidential and are consistent with MD 12.2, “NRC Classified Information Security Program.”

- a. **Classified National Security Information.** Information that has been determined pursuant to Executive Order 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 the “Atomic Energy Act of 1954,” as amended (AEA), Section 142, “Classification and Declassification of Restricted Data” **(42 U.S.C. 2162).**

02.03 **Safeguards and** Sensitive, Unclassified Information

This section includes Safeguards Information (SGI), Safeguards Information-Modified Handling (SGI-M), and Sensitive Unclassified Non-Safeguards Information (SUNSI). Refer to **internal website** <https://usnrc.sharepoint.com/sites/SUNSI> for more information on SUNSI, including Personally Identifiable Information (PII) and pre-decisional enforcement information.

Note: The NRC is currently in the process of transitioning from the agency’s SUNSI program to the governmentwide **Controlled Unclassified Information (CUI)** program established by Exec. Order No. 13556, “**Controlled Unclassified Information,**” and

implementing regulations from the National Archives and Records Administration in Title 32 of the *Code of Federal Regulations* (CFR), Part 2002, “**Controlled Unclassified Information (CUI)**.” Refer to **internal website <https://usnrc.sharepoint.com/sites/NRC-CUI-Program>** for more information on the **status of NRC’s transition to CUI**. Continue to use existing SUNSI guidance until the NRC fully implements the CUI Program.

- a. **Safeguards Information (SGI)**. Refer to 10 CFR 73, “Physical Protection of Plants and Materials,” Section 2, “Definitions,” and 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. **Sensitive Unclassified Non-Safeguards Information (SUNSI)**. Refer to **internal website <https://usnrc.sharepoint.com/sites/SUNSI> for more information**. SUNSI is defined as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and federal programs, or the personal privacy of individuals. This includes, among other things, proprietary information obtained from a licensee, security-related information that does not qualify as SGI or classified information, PII, and NRC pre-decisional information.
- d. **Official Use Only-Security Related Information (OUO-SRI)**. **If an NRC licensee requests inspection procedures (IPs) or other regulatory guidance documents that are OUO-SRI, the NRC staff can share those IPs or regulatory guidance documents with the licensee, provided a need to know is established, and the documents are transmitted through an NRC-approved secure method.**

02.04 Document Types

- a. **Licensee, Vendor, or Applicant-Controlled Document**. Any document, correspondence, email, 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, email, or information that requires special handling to restrict access or disclosure. These include documents that contain classified information, SGI, SGI-M, and SUNSI.

- 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. **Background information, when included in such drafts, is considered non-record documentary material provided it does not form the basis of an inspection finding or enforcement action.**
- 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 or electronic 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)

Federal law that establishes the right of any person to obtain access to agency "records," as defined by the Act, unless the records or portions thereof are protected from public disclosure by one of nine exemptions (Refer to MD 3.1, "Freedom of Information Act," and 10 CFR Part 9, "Public Records"). Documents are considered "agency records" for purposes of FOIA if they are created or obtained by the NRC and under the "control" of the NRC at the time a FOIA request is made.

When evaluating whether the NRC controls a record, the following are taken into consideration: whether the licensee has intended to relinquish control of the document to the NRC; the ability of the NRC to use and dispose of the document as it sees fit; the extent to which the NRC has relied upon the document; and the degree to which the document has been integrated into the NRC's records or files in the course of official agency business. As stated in Section I.B.1 of the Handbook to MD 3.1, "[t]o be under the control of the agency, the record must have come into the agency's possession through the legitimate conduct of its official duties."

For the purpose of the FOIA, records include "any information that would be an agency record ... when maintained by an agency in any format, including an electronic format" such as the following:

- paper records
- audiotapes
- videotapes
- TEAMS chat messages
- email
- photographs
- books
- microfiche and other machine-readable formats

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 website, if not downloaded to an NRC controlled network or printed, are not considered to be in the possession and control of the inspector. **Internal Form 1150, "Employee Estimate/Search in Response to FOIA Request," can be used when collecting FOIA information from staff and to maintain a record of searches and responses.**

Any records withheld from a FOIA request must be retained for a period of 6 years from the denial date despite the disposition schedule in NUREG-0910, "NRC Comprehensive Records Disposition Schedule" (see MD 3.1, Section I.B.4.c, "Retention of Records"). The FOIA coordinator in your office should be contacted if there are questions about retention for records related to a FOIA request.

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 on site). 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.

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 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 **and Similar Materials**

Working files (such as preliminary drafts and rough notes) and other similar materials, are generally temporary records that **must be** maintained to ensure adequate and proper documentation until used to create a longer-term record, **until** superseded by development of another record, or **until** no longer needed, such as to preserve a complete understanding or explanation of an agency action or decision (36 CFR 1222, "Creation and Maintenance of Federal Records"). **The files meet the following parameters: "(1) [t]hey were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action, recommendation,**

follow-up, or to communicate with agency staff about agency business; and (2) [t]hey contain unique information, such as substantive annotations or comments that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.” Examples of working files created by an inspector include but are not limited to: (1) written or electronic notes; and (2) written or electronic notes taken on copies of licensee, vendor or applicant documents, and calculations. These notes or files are often created and used during the course of an inspection and aid in the implementation of an inspection and the creation of an inspection report. Note: Most inspection-related working file records are short lived and do not ultimately go into ADAMS. Refer to Section 04.04a in this IMC 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 or electronic 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 may be treated as a federal record. The use of a label such as “personal” does not control the status of documents 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 they believe to be personal records, these records are reviewed by the employee using NRC Form 510, “Personal Records Checklist,” to determine if the records are personal or agency records. Examples of agency records may include email correspondence to/from a personal email account related to agency business. If determined that the records are personal, the employee provides the completed Form 510 and the personal records 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

Information obtained from a person outside the federal government that consists of (1) trade secrets, or (2) commercial or financial information, and which the person treats as privileged or confidential. Proprietary information that is submitted to the NRC must comply with the document marking and affidavit requirements set forth in subsection (b) of 10 CFR 2.390, “Public inspections, exemptions, requests for withholding,” in order for the NRC to treat the information as proprietary and withhold from public disclosure. Refer to <https://usnrc.sharepoint.com/sites/SUNSI> (non-Public) 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, “What Definitions Apply to the Regulations in Subchapter B?”)
- 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 and 1222.10).

Records created (e.g., copying or printing licensee documents) by the NRC inspector, or reproduced by any means (e.g., inspector written notes), could be considered federal records if preserved or determined appropriate for preservation by 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 (for example, name, Social Security number, passport/visa number, or assigned case number). (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.”) See Section 02.06 for special considerations regarding FOIA records.

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 is granted to inspectors in a manner equivalent to access provided to 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 in this document.

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 and implement existing policies, guidance, and regulatory requirements for the collection, acquisition, control, and disposition of documentation used in preparing for inspections, gained during the conduct of inspections, and resulting from inspections.
- b. Ensure appropriate corrective actions are taken and notifications made when inspection documents are released contrary to NRC policies, procedures, regulations, and legal requirements.

03.03 Inspector Supervisors

- a. Ensure that their staff is cognizant of, adheres to, and implements existing policies, guidance, and regulatory requirements for the collection, acquisition, control, and disposition of documentation used in preparing for inspections, gained during the conduct of inspections, and resulting from inspections.
- b. Take appropriate corrective actions and make required notifications to the Cybersecurity Incident Response Team (CSIRT) when inspection documents are released contrary to NRC policies, procedures, regulations, and legal requirements. Additional information concerning information spills can be found in MD 3.4 and 12.5, "NRC Cybersecurity Program."
- c. Review and approve docketed notification of inspection and request for information (RFI) correspondence letters and ensure that information requests are compliant with the Paperwork Reduction Act (PRA). For questions concerning PRA requirements for an RFI, contact the FOIA, Library, and Information Collections Branch (FLICB) in the Office of the Chief Information Officer (OCIO), Data, Information Management, and Enterprise Governance Division (DIME).

03.04 Inspectors

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

0620-04 BASIC REQUIREMENTS

The NRC generates and receives many categories of documents and emails containing SUNSI. Inspectors are responsible for properly handling, marking (including portion marking when applicable), and protecting from unauthorized disclosure of SUNSI. See NRC's internal webpage for additional guidance (<https://usnrc.sharepoint.com/sites/SUNSI>).

04.01 Requesting, Obtaining, **Sharing**, Reviewing, and Disposing of Inspection-Related Information

a. Requesting Documents as Part of Inspection Preparation.

Specific responsibilities and procedures that comply with the Paperwork Reduction Act (PRA) of 1995 are found in MD 3.54, "NRC Information Collections Program" and in YA-24-0072, "Paperwork Reduction Act Requirements" (non-public).

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. **Be cognizant of concurrent RFIs from other NRC entities. See the Office of Management and Budget's (OMB's) regulations in 5 CFR Part 1320, "Controlling Paperwork Burdens on the Public."**
 2. Inspectors should not request documents that already exist as NRC official records in ADAMS.
 3. **Requests must be tailored to the specific inspection scope and limited to information necessary to meet inspection objectives. Inspectors shall ensure that information requests are directly linked to the specific inspection population, selected samples, or applicable inspection attributes.**
 4. 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 email 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 **for this purpose** 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. **These types of written or electronic requests are official records and should be placed in ADAMS.** Documents received through this process may become part of the working file or inspection record which would be subject to FOIA requests.
- Resident and senior resident inspectors should periodically communicate to appropriate licensee staff **regarding** the types of documents they will routinely use for inspection; **also communicate that those documents** may routinely be under NRC possession and control and **thus may be** subject to **possible release via a FOIA request**.
5. **The branch chief responsible for the inspection shall review the initial documentation request to ensure it meets the IMC 0620 guidance.**
 6. Corresponding with the licensee, vendor, or applicant via email or phone is an appropriate method to request additional documents.
 7. Documents that contain classified information (i.e., National Security Information and Restricted Data) may not be transmitted via email. SGI may not be emailed over an unprotected network unless the files are encrypted on an SGI system using a **version**

of Pretty Good Privacy software that is compliant with Federal Information Processing (FIPS) Standard Publication 140-02 (or later), "Security Requirements for Cryptographic Modules" (FIPS 140-2 was superseded by FIPS 140-3 effective September 22, 2019); the files would then be transferred in encrypted form to the local area network for email transmission. (Refer to MD 12.2, MD 12.4, "NRC Communications Security (COMSEC) Program," and MD 12.7 "NRC Safeguards Information Security Program," for the current policy). SGI and Confidential information 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 encompasses a wide variety of categories (e.g., personal privacy, allegations, pre-decisional, proprietary etc.) handled according to the requirements found on the [internal SUNSI website](#).

8. Email may be used for transactional purposes with licensees to exchange general information on administrative activities (such as schedules, meeting preparations, and travel plans), or to request additional documents for review during inspection activities. These emails must be sent from NRC accounts or be courtesy copied (cc'd) or forwarded to an NRC account within 20 days. So long as these emails do not contain agency positions, draft conclusions, or otherwise provide evidence of agency decision-making, they typically do not need to be placed in ADAMS. See Section 04.02.c.2 in this IMC for guidance on controlling the information if technical communications and/or questions are communicated during inspection preparation.
9. Letters or emails requesting inspection information at the beginning of the inspection from the licensee, vendor, or applicant should include a PRA statement which includes a valid OMB control number. Refer to Exhibit 2 for a sample PRA statement. To ensure compliance with the PRA, the author should verify the accuracy of their PRA statement by contacting the Information Collection Team in OCIO.

b. Obtaining and Sharing Documents During Inspection Activities.

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, or 10 CFR 70.55 exists or if actions should be taken under Section 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. This includes the use of file sharing services. (See Section 04.01.b.8 **below** for additional information).
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 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 disclosure if subject to a FOIA request.
8. **SharePoint external sharing (SPxS) is the NRC's solution for external sharing of business-necessary content by authorized staff with registered external parties. SPxS replaces the Box.com service which retired in September 2025. Staff have the responsibility to protect sensitive NRC information, as directed in non-public Yellow Announcement (YA) 20-0044, "Use of External File Share Services," and MD 12.5. Access to SPxS and the NRC External Collaborator app is reserved for NRC staff who have taken training, acknowledged the Rules of Behavior, and requested and obtained an external SharePoint site. In addition to staff registration, there is a process for external user registration to view or download documents; permissions for external access are set in SharePoint. Further information on External Sharing is available at [NRC External Collaboration](#) (non-public site). The SPxS site has been approved as the agency's file sharing solution for SUNSI. No other solution shall be used for NRC-initiated file sharing of business information. Note that licensees need**

to place materials in their own portal if they want to retain ownership of those materials.

In cases where an external entity such as a licensee or another agency initiates an invitation to a file sharing services (other than SPxS), this non-NRC portal may be used to collaborate only on non-NRC information. When receiving an invitation from an external entity, register an account using your NRC email 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 (PII), 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 2.6, “Information Technology Infrastructure and End User Services.”

<u>NRC Work-Related</u>				
<u>Activity</u>	<u>Solution</u>	<u>Audience</u>	<u>Email Account</u>	<u>Information Type</u>
Sharing NRC data	NRC Collaborator app	Licensees, Contractors, or NRC staff	NRC	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 2.6, “Information Technology Infrastructure and End User Services”	Self or someone else	Personal	Personal data

Note: NRC inspectors should inform licensees that documents obtained during the course of an inspection may be “agency records” subject to release under the FOIA. 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 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 of this IMC. 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 Documents and Records During Inspection Activities

a. Draft Documents & Other Information

1. In preparation for or during inspections, inspectors should normally request only those documents that have completed the licensee's or vendor's required review and approval process; those documents 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 relate to immediate safety concerns or issues, such as compensatory measures taken to address equipment operability or other issues that are time sensitive. The licensee may choose to provide draft information to a Senior Risk Analyst (SRA) to support timely and accurate risk assessments. Inspectors should not act as a licensee consultant when reviewing draft documents.

NRC staff may review and comment on draft licensee documents prior to formal submission only when necessary to support regulatory responsibilities. Such reviews must avoid any real or perceived impropriety or preferential treatment and should be based solely on regulatory need. NRC-initiated reviews may also be appropriate when draft documents serve the agency's public health and safety mission, such as those that:

- assist with inspections or assessments of corrective actions,
- could form the basis for a confirmatory order, or
- support a settlement agreement

Any document obtained from a licensee which the licensee indicates is a draft, should be clearly marked and handled as such.

Any document, including those labeled "drafts," considered by the staff in reaching a regulatory decision should generally be placed in the appropriate docket file and in ADAMS.

Examples of When to Retain or Dispose of Draft Documents

- (a) Early in an inspection, an inspector reviews a draft procedure change to verify that changes committed to in response to a violation are being incorporated.

Retention not required: The draft served only as background information. The final, issued procedure will document completion of corrective actions in response to the violation.

- (b) During an in-field observation of work in progress on an electrical modification, the inspector reviews the related mark-up drawings and proposed procedure changes to be sure appropriate modification and work control procedures are being followed. No discrepancies were identified by the inspector relating to control of the modification or work.

Retention not required: The drafts provided the background necessary to assess the licensee's adherence to the appropriate modification and work controls.

(c) During a similar situation to Example 2 above, the inspector notes that the mark-up drawing (draft) indicates that the as-installed configuration of the modification violates electrical separation requirements. The electrical separation requirement violation is confirmed by direct observation by the inspector.

Retention required: The draft mark-up drawings, along with the inspector's observation, supports an inspection finding and enforcement action. The draft may not be retrievable from the licensee later.

(d) The inspector reviews an electrical analysis under development by the licensee's engineering organization as part of the assessment on the quality of the licensee's corrective action process.

Retention not required: The focus of the inspection was on the process used by the licensee in performing the analyses, not on the results of the analyses.

2. 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. Consider that the licensee or vendor may feel compelled to generate documents to satisfy the inspector's request. This could impose a backfit as well as an unnecessary burden on the licensee or vendor if there is no regulatory requirement for the documents or analyses requested. See Management Directive (MD) 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests."
3. 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.

b. Use of Cameras and Recording (Including Video) Devices

1. Inspectors should ensure that the licensee, vendor, or applicant is made aware that inspectors may be taking photographs or video recordings during the course of their normal inspection activities. Photographs or video recordings should be taken from NRC issued devices. In instances when this does not occur, they should be forwarded to an NRC account within 20 days.
2. Inspectors should verify that the licensee, vendor, or applicant is not recording any virtual meetings as part of interactions during inspection activities. If recording is made, the inspector should consult with regional counsel.
3. Inspectors **should** openly communicate and observe all established licensee, vendor, or applicant procedures for photography or recording. The licensee, vendor, or applicant may not impede or interfere with inspections by limiting the use of NRC cameras or recording devices (See Section 235 of the AEA). Sensitive photographs or recordings requiring protection under 10 CFR 2.390 should be appropriately marked. Photographs or recordings containing sensitive information should be properly designated by inspectors prior to transmitting off site.

4. Refer to Exhibit 1 for further guidance on the use of photographs or videos during the inspection process.

c. Written Notes and Electronic Correspondence

1. Handwritten notes to licensee, vendor, or applicant should, to the extent possible, only communicate general information on administrative activities or to request specific documents associated with the inspection when on site.
2. Email may be used to provide questions to licensee, vendor, or applicant as part of inspection activities. These emails must be sent from NRC accounts or be **courtesy** copied (cc'd) or forwarded to an NRC account within 20 days and should not contain draft agency position or inspection conclusions. Emails seeking to clarify information regarding ongoing technical aspects identified by an inspector in the course of an inspection do not typically need to be placed in ADAMS. However, such emails, as well as any response received via email, should be reviewed on a case-by-case basis pursuant to MD 3.53, "NRC Records **and Document** Management Program," to determine whether they are appropriate for preservation in ADAMS as a federal record (44 U.S.C. 3301). Staff should assess whether such emails would serve as evidence of NRC decisions not otherwise contained in the inspection report. If determined not to be federal records, they should be controlled as part of the working file and can be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. Inspectors should be aware that working files and licensee, vendor, or applicant responses may be subject to the FOIA while they are in the agency's possession and control.
3. Written or electronic notes created by the inspector can be considered as 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/electronic notes shall not be shared with the licensee.

d. Team Meetings, Licensee, Vendor, or Applicant Debrief, and Exit Meetings

1. 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.
2. 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).
3. A written or electronic list of preliminary inspection findings should not be given to licensee, vendor, or applicant management. However, if it is necessary to give to the licensee, vendor, or applicant, see Section 04.04.b.6.

e. Storage and Disposal of Inspector Written Notes and Materials

1. 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 should be done at an NRC facility. (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.)
2. 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.
3. 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 resident inspector's office.

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

1. 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.
2. 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.
3. 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 the 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 may 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. The inspector should not use these forms to provide questions. 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 responses can be reviewed by the inspector during the onsite inspection.
2. Electronic responses by the licensee to questions emailed by the inspector during the course of an inspection can be considered 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. However, such email responses should be reviewed on a case-by-case basis pursuant to MD 3.53 to determine whether they are appropriate for preservation in ADAMS as federal records (44 U.S.C. 3301). Staff should assess whether such emails would serve as evidence of NRC decisions not otherwise contained in the inspection report.

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 modeling 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). This includes, 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 inspector should promptly report the unauthorized disclosure to their supervisor. Refer to MDs 3.4, 3.5, "Attendance at NRC Staff-Sponsored Meetings," and 12.5 for further actions and additional 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 addressed in accordance with the applicable MD.

5. If email 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 email groups, which only contain NRC staff members, is encouraged to reduce the risk of MS Outlook sending email to unintended recipients by using the auto-complete function.
6. Existing technologies, such as shared internal drives, **OneDrive**, SharePoint, or Teams, are alternate ways to communicate sensitive information versus email. When used properly, these methods can ensure that only those within the NRC have access to the information. 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 (**or ADAMS link**) in their NRC staff group email.
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.

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, email, 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). Common exemptions that may apply to agency records in the context of inspections are Exemption 1 (classified information); Exemption 3 (SGI); Exemption 4 (proprietary information obtained from the licensee); Exemption 5 (agency pre-decisional and deliberative information); Exemption 6 or 7(C) (personal privacy information); or Exemption 7(F) (information that, if released, could reasonably be expected to endanger the life or physical safety of any individual).
- c. In the event of a FOIA request that includes agency records obtained or created during the course of an inspection that, if disclosed, would reveal a licensee's trade secrets or confidential commercial or financial information, the NRC is obligated to provide the submitter of that information with an opportunity to object prior to any such disclosure. See 10 CFR 9.28. This can include any information obtained from the licensee, as well as NRC-generated records that incorporate such information, including photographs or videos taken by NRC inspectors.

It is important that staff be fully versed in the FOIA process to avoid inadvertently destroying records that are currently included in an active or recent FOIA search.

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. 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 email 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 or 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. 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.

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. Documents in the list below are required to be declared as records and placed in ADAMS. Documents **such as the following**—SGI (typically stored in the SGI local area network electronic safe (SLES)), pre-decisional enforcement documents, and allegations files—are not placed in ADAMS.

1. Written correspondence (including emails and faxes) from the licensee, vendor, or applicant that formally responds to a regulatory decision (that is, findings, significance determination, or licensing action).
2. Team inspection notification and document request letters generated per Section 04.01a.5.
3. NRC 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 (that is, findings, significance determination, or licensing action).
5. Unique documents or excerpts of documents that cannot be recreated by the licensee, vendor, or applicant that were used to substantiate a regulatory decision (that is, 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 (for instance, a 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), “**Public inspections, exemptions, requests for withholding**”; the exceptions to the definition of “agency record” found in 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. Documents and records which are not retained and contain sensitive unclassified information must be destroyed in a manner which prevents reconstruction of the information (for example, **securely** shredded). Sensitive unclassified information may also be placed in receptacles designated for classified waste or approved for sensitive unclassified **materials**. For further information on document destruction, see the SUNSI Handling Requirements **found in the [internal SUNSI SharePoint site](#)**. For information on handling classified information or SGI, see MD 12.2 or MD 12.7.

0620.05 REFERENCES

5 CFR Part 1320, “Controlling Paperwork Burdens on the Public”

10 CFR 2.390, “Public inspections, exemptions, requests for withholding”

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

10 CFR 73, “Physical Protection of Plants and Materials”

32 CFR Part 2002, "Controlled Unclassified Information (CUI)"

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

36 CFR 1237.28, "What special concerns apply to digital photographs?"

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

Exec. Order No. 13526, "Classified National Security Information"

Exec. Order No. 13556, "Controlled Unclassified Information"

Form 1150, "Employee Estimate/Search in Response to FOIA Request" (non-public)

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

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 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"

MD 2.6, "Information Technology Infrastructure and End User Services"

MD 3.1, "Freedom of Information Act"

MD 3.2, "Privacy Act"

MD 3.4, "Release of Information to the Public"

MD 3.5, "Attendance at NRC Staff-Sponsored Meetings"

MD 3.53, "NRC Records and Document Management Program"

MD 3.54, "NRC Information Collections Program"

MD 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests"

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 Communications Security (COMSEC) Program"

MD 12.5, "NRC Cybersecurity Program"

MD 12.7, "NRC Safeguards Information Security Program"

NUREG-0910, "Comprehensive Records Disposition Schedule"

Exhibit 1: Use of Photographs or Videos During Inspection or for Informal Training

USE OF PHOTOGRAPHS OR VIDEOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	Additional Information
1. Should I inform the licensee, vendor, or applicant prior to taking photographs or videos?	<p>The licensee, vendor, or applicant should be made aware that the NRC may be taking photographs or videos during all inspection activities.</p> <p>Requests by the licensee, vendor, or applicant to review photographs or videos for personal privacy, classified, proprietary, or safeguards information should normally be honored.</p> <p>Use common sense in taking photographs or video as part of your routine inspection activities. Avoid taking photographs or videos of personnel or plant or facility features related to security when irrelevant to the inspection or photographs or videos that unnecessarily contain sensitive information. Follow the licensee's policy on the use of photographic and video equipment.</p>	IMC 0620 Sections 02.13.a and 04.02
2. What if the licensee, vendor, or applicant objects to taking photographs or videos?	<p>All licensee objections should be considered seriously. If photographs or videos contain sensitive information, such as SGI or SUNSI, they should be appropriately marked and controlled in accordance with law and NRC policy. Inspectors will often need to use photography or video to effectively document inspection-related agency decisions and actions. Objections to photography or videos 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 or video devices. Inspectors should share any licensee's, vendor's, or applicant's concerns with their regional management when objections are raised.</p>	
3. Can I forward photographs or videos to my management electronically without the licensee's, vendor's, or applicant's review?	<p>Yes, after the photograph is appropriately designated and 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 designation when deemed appropriate. Inspection-related photographs or videos should be controlled to prevent improper or unauthorized public disclosure.</p>	IMC 0620 Sections 02.13b and 04.03c

USE OF PHOTOGRAPHS OR VIDEOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	Additional Information
4. Do I need something in writing from the licensee, vendor, or applicant that says it has reviewed the pictures or videos for classified, safeguards, and SUNSI information?	No. However, requests by the licensee, vendor, or applicant to review photographs or videos for classified, safeguards, or SUNSI (personal privacy or proprietary information) information should normally be honored so as to ensure proper designation. Photographs or videos that include sensitive information must be controlled in accordance with law and agency policy.	
5. Is there agency guidance on how to forward photographs or videos that contain classified or sensitive unclassified information?	<p>Yes. Photographs or videos that contain proprietary information or other kinds of SUNSI can be forwarded electronically (via email or other internal file sharing application). Photographs or videos that contain unencrypted classified or SGI cannot be forwarded via email over an unapproved network .</p> <p>Also, all photographs or videos believed to contain classified information, SGI, or SUNSI 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>IMC 0620 Section 04.01a5 MDs 12.2 and 12.4.V.C, SUNSI FAQ (non-public)</p>
6. How do I know when photographs or videos must be retained?	<p>If the photographs or videos are used to substantiate an inspection finding and they do not contain classified or safeguards information, they should be retained and placed into ADAMS. Photographs or videos that reveal SUNSI, such as proprietary information or personal privacy information, should be placed in non-public ADAMS.</p> <p>Examples of photographs used to substantiate an inspection finding include photographs or videos 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>IMC 0620 Sections 02.01, 02.13a, 04.04b</p> <p>NRC authority under the Atomic Energy Act of 1954</p>

USE OF PHOTOGRAPHS OR VIDEOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	Additional Information
7. When are photographs or videos required to be destroyed?	<p>If the photographs or videos are not used to substantiate an inspection finding, they may be destroyed in accordance with NRC guidance for working files.</p> <p>Examples of photographs not used to support an inspection finding include: (1) those photographs or videos that are used as memory joggers to assist the inspector in finalizing the inspection report and (2) photographs or videos forwarded electronically to regional management to clarify or to discuss findings. Photographs or videos of this nature generally are not relied on for regulatory decision-making.</p>	IMC 0620 Section 04.04a
8. 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 (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>10 CFR 2.390(b)(1) 10 CFR 9.28</p> <p>MD 12.1</p> <p>Guidance for Determining the Public Availability of NRC Records (ML072770468)</p>
9. If photographs or videos are not used to support inspection findings, can they be retained for training purposes?	<p>If the photographs or videos do not contain classified, safeguards information, or SUNSI (personal privacy or proprietary), they may be retained for informal training purposes.</p> <p>If the photographs contain classified, safeguards information, or SUNSI (personal privacy or proprietary), then they should be destroyed unless such information is absolutely necessary to support formal training objectives.</p>	NRC authority under the Atomic Energy Act of 1954

USE OF PHOTOGRAPHS OR VIDEOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	Additional Information
10. Do I need the licensee's, vendor's, or applicant's permission to keep these photographs or videos for training purposes?	<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. However, it is a good practice to seek permission from licensee, vendor, or applicant.</p> <p>Requests by the licensee, vendor, or applicant to review photographs for classified, safeguards, or SUNSI (personal privacy or proprietary information) information should normally be honored to ensure proper designation.</p>	NRC authority under the Atomic Energy Act of 1954
11. Are training photographs or videos subject to FOIA?	Yes. Photographs and videos in the possession of the NRC even if used for training purposes (including the Inspector Newsletter) are subject to FOIA.	MD 3.1
12. How should the photographs or videos be identified when used for training purposes?	Photographs or videos that contain proprietary information must be labeled as such in accordance with the NRC's SUNSI policy and should include the date and name of the facility or facility owner. Photographs should be documented and designated as they are produced.	<p>10 CFR 2.390</p> <p>36 CFR 1237.28, "What special concerns apply to digital photographs?"</p>
13. If the photographs or videos contain classified and safeguards information, can they still be used for training purposes?	Yes, Staff reviewing such photographs must possess the appropriate clearance levels and have a "need to know." If this is the case, such photographs and videos and digital devices that contain classified and safeguards information must be secured and agency guidance followed.	<p><u>SUNSI</u> (non-public)</p> <p>MDs 12.1, 12.2, and 12.7</p>
14. Are photographs or videos used for training purposes required to go in ADAMS?	<p>No, if the photographs or videos are used for informal training (on the job training (OJT) and learning opportunities). Yes, if the photographs or video are used for formal training (e.g., Technical Training Center).</p> <p>Note: SGI photographs or videos would be stored on the SLES or on another approved storage location for training.</p>	MD 3.53

USE OF PHOTOGRAPHS OR VIDEOS DURING THE INSPECTION PROCESS

QUESTION	ANSWER	Additional Information
15. How long should photographs or videos used for informal training (OJT and learning opportunities) be retained?	Photographs or videos should be destroyed when they are no longer needed.	
16. How long should photographs or videos 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 FOIA, Library and Information Collection Branch, Office of the Chief Information Officer, Mail Stop: T6-A10M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-XXXX) OMB, 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.

Note: The estimated burden can be based on the following formula:

For every 5 hours of direct inspection effort, there is an estimated 1 hour of information collection burden (rounded up to the nearest integer). Inspectors can adjust the estimate up or down based on perceived scope of the information request, as not all information requests will be equivalent.

Note: Per 10 CFR 52 (72 FR 49352), oversight of nuclear plants licensed under Part 52 is governed by 10 CFR 50. As such, the Part 50 OMB control number should be used for oversight of nuclear plants licensed under Part 52.

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 email 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	N/A	N/A
N/A	ML21089A217 07/09/21 CN 21-023	Updated to reflect current practices on use of email by inspectors during the course of an inspection. Other minor editorial changes to streamline, remove redundancy, and better clarify content.	N/A	ML21098A076
N/A	ML25218A214 02/20/26 CN 26-007	Completed 5-year review. Restored reference column in Exhibit 1. Updated FOIA section; clarified records subject to FOIA. Updated references throughout. Updated definition of working files. Added instruction to calculate the estimated burden for PRA statement. Included a voluntary list of standards and expectations for licensee information sharing with NRC inspectors based on the 2022 Follow-On Review Lessons Learned During COVID (Recommendations 5 through 8 and 11). Updated external file sharing from Box to SPxS. Incorporated contents of IMC 0330 (now deleted).	N/A	ML25219A266