The Freedom of Information Act (FOIA)

Stephanie Blaney
FOIA Officer
Information Services Branch
Office of the Chief Information Officer
September 26, 2018

The Freedom of Information Act Agenda

Topic	Presenter	Time Allotted
• Welcoming Remarks	Dave Nelson, CIO/Scott Flanders, Deputy	5 mins
• Overview of FOIA	Stephanie Blaney, FOIA Officer	10 mins
• FOIA Fee Estimates and Search	Margo Stevens, Contractor	20 mins
• Records	Margie Janney, Chief/Records Officer	15 mins
• Draft documents	James Adler, OGC/Senior Attorney	20 mins
• CEII	Andy Campbell, NRO/DLSE Deputy	20 mins
• Q&A Session		

The Freedom of Information Act

FOIA is a law that gives any person the right to request federal agency records.

FOIA pertains to federal agency records that exist and can be located in the agency files.

The Freedom of Information Act

- Who?

Any person

- Individuals
- Corporations
- Associations
- State and local governments, etc.

The Freedom of Information Act

- What?

Paper records

Emails

Audio/voicemails

Video

Electronic

FOIA Perfected Request

- Request in writing
- Reasonably described
- In compliance with agency regulations

Forms for FOIA

- Form 496 - Report of Staff Resources for Processing FOIA requests
- Form 496A – Referral of Records Related to a FOIA request
- Form 511 – Program office response to a FOIA request

Forms for FOIA continued

- Form 511A – Documentation of FOIA search
- Form 510 – Personal Records checklist

Tracking FOIA Time

- HRMS Reporting Code – ZF0000

Questions

You've been tasked with a FOIA…

now what do you do?

Margo L. Stevens

FOIA Analyst/Team Leader (QualX Corp. contractor)
Information Services Branch
Governance & Enterprise Management Services Division
Office of the Chief Information Officer
September 26, 2018

FEE ESTIMATE

What goes into a Fee Estimate?

- Carefully read the FOIA request; ensure you understand what is being asked for.
- With your office's FOIA Coordinator and any other SMEs, decide whether any clarification or scope narrowing is appropriate.
- Pay attention to the requester's fee category. Provide only what is asked for.
  - Commercial use: review, search and duplication
  - Favored (media, educational or scientific institution): duplication > 100 pages
  - Non-excepted (other): search > 2 hours and duplication > 100 pages

What goes into Search Time?

- Time spent looking for material subject to a request, either manually or by automated means, including the time spent in page-by-page or line-by-line identification of responsive material within multi-subject records.
- If multiple SMEs will be contributing to the fee estimate, ask your office's FOIA coordinator to designate someone to search shared spaces (e.g., ADAMS, Sharepoint, shared drives).
- Each SME should search personal space (e.g., hard copies kept in your office, electronic copies on your computer (*e.g.*, all drives, Outlook), CDs/DVDs, and flash drives).

What goes into Review Time?

- The time spent during the initial examination of a record to determine whether material may be withheld, including the time spent bracketing or describing such material.
- It does not include time spent resolving general legal or policy issues about whether to apply a particular exemption (*e.g.*, conferring with your management, seeking legal advice from OGC, or determining foreseeable harm).

Keep in mind….

- Arriving at the “sweet spot”
  - ✓ We don’t want to overstate the time so as to appear to be discouraging the requester from pursuing the request
  - ✓ But we don’t want to understate the time either so that the requester is surprised at the bill received at the end
- Make sure your office’s FOIA coordinator knows whether you are an (1) executive; (2) professional (manager or technical); or (3) administrative/clerical staff member as the fee rates differ.
- Many requests don’t end up with billable fees (not that we grant fee waivers).
- Since the FOIA Improvement Act of 2016, agencies cannot charge search or duplication fees if responses are late. (We can still charge commercial use requesters review fees.)

Search and Review

Conducting Your Search

- As with the fee estimate, if multiple SMEs in your office are involved, your office's FOIA Coordinator should consider holding a meeting to ensure alignment on the request's interpretation, who will search shared sites, and provide any other instructions.
- Remember to provide records in their native format.
- You can provide records electronically or in hard copy.
- Even if you're aware of previous FOIA requests for the same records, you will have to search again if the earlier requests > 6-year retention schedule or there are records created after the earlier requests' cut-off date.

The “Three C’s”

Complete, Clear and Concise

COMPLETE

- Make sure all attachments "travel" with the email, memo, or letter to which they are attached.
  - ✓ Do not separate them, even if your disclosure recommendation is different.
  - ✓ If the same material is attached to multiple emails, you need only produce it once (but be sure that your office's FOIA Coordinator understands this, so it can be conveyed to the assigned FOIA specialist).
- Provide a particularized foreseeable harm statement for any deliberative process or security-related material.
- Provide a description of how/where you searched for records. (You may use Form 511A for this purpose.)

COMPLETE, cont'd.

- Proprietary Records
  - ✓ If a licensee included a 2.390 affidavit, provide it (or its ML#)
  - ✓ Indicate whether you agree that all of the material is proprietary (or indicate what material may be released)
  - ✓ Provide the name, telephone #, and email address for the licensee (or other business submitter)'s point of contact

CLEAR

- Instead of bracketing and marking exemptions on each page (or portion), consider whether you can simply describe the material you're recommending be redacted and the exemption you believe applies.
  - ✓ This is less work for you and the assigned FOIA specialist (since all those brackets/markings need to be erased before a final response is issued).
- Use only these groupings: (1) a listing of any records already publicly available in ADAMS; (2) a listing of any records for which the assigned FOIA specialist will need to have their profiles changed to publicly available; (3) records processed (RIF, RIP, or WIF); and (4) records to be referred (for which you have no equities).

CONCISE

- De-duplicate!
  - ✓ Every SME, office FOIA Coordinator, and assigned FOIA specialist is expected to de-duplicate records
    - The final page and the concurrence page are not duplicates.
    - For emails, start by using Outlook's "Clean Up" functionality to eliminate duplicates. A shorter email string that appears, in its entirety, in a longer email string is considered a duplicate (so long as you don't lose any attachments).
- Please do not staple, paper/binder clip, or affix post-it notes or flags on, pages. (if you must 'bind' pages together, please use rubber bands).

A Final Tip

- Where practicable, keep a copy of the records you've processed until your office's FOIA Coordinator receives notification that the FOIA request is closed.
  - ✓ If the assigned FOIA specialist, FOIA Officer, or OGC attorney reviewing a response has questions, you'll have the record to refer to.
  - ✓ If the requester submits an appeal, you'll have the record to refer to if you're asked to reconsider whether to still claim an exemption
  - ✓ If the records were uploaded to the FOIA Office's Sharepoint site, or a shared drive, then you needn't keep your own copy.

Any Questions?

Records Management in a FOIA World

September 26, 2018

Margie Janney, CRM/NS/FED
Agency Records Officer
Chief, Information Management
Services Branch
OCIO

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RM in a FOIA World

- What are Federal Records?
- FOIA vs Federal Records Act (FRA)
- Records Management Responsibilities
- Retention of FOIA Records
- Questions

FOIA vs. FRA

- The purpose of FOIA is to provide the public with access to Federal records explaining Government operations.
- The purpose of the Federal Records Act (FRA) is to provide the legal framework for federal records management, including records creation, maintenance, and disposition.

What are Records under the FRA?

Short Definition

- All documentary materials, regardless of physical form or characteristics, made or received under Federal law or in transacting Government business.

See Federal Records Act (FRA), 44 U.S.C. 3301

Key Points

- It does not matter what the media is, **it is the information that matters.**
- Federal records are not only those things **created within** the agency, but are also items **received from the outside**.
- Records are kept for varying lengths of time because they have information in them that is **useful for short, medium, or long periods of time and are used for operation, legal, fiscal, or historical purposes.**

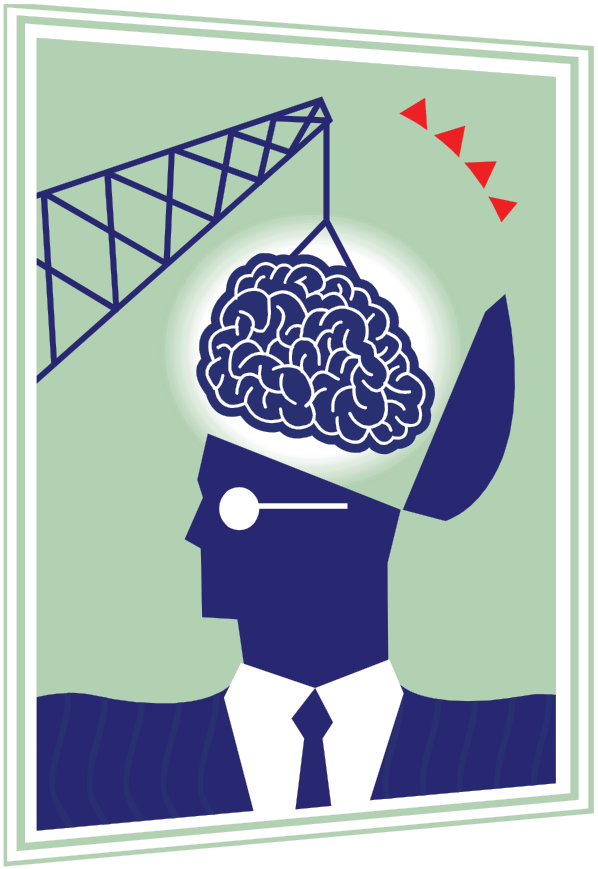
Records Management Responsibilities

- Document NRC business in agency records
- Retain agency records for the retention period
- Dispose of records at the end of the retention periods unless they are the subject of a current FOIA request or litigation hold

Retention of FOIA Records

- Offices do not need to keep copies of their FOIA response once the case is closed.
- Retention of FOIA case files is the responsibility of the FOIA Team
  - 6 years

QUESTIONS?



Margie Janney
301-415-7245

IT/IMPolicy.Resource@nrc.gov

DRAFTS AND FOIA

How to treat draft documents that are responsive to FOIA requests

James Adler
Office of the General Counsel
FOIA Annual Training – September 2018

FOIA Exemptions And Drafts

- If a non-public draft document is responsive to a FOIA request, a range of FOIA exemptions could conceivably apply, which could either permit or require withholding of the document in whole or in part.
- First, there may be reasons for withholding that are *not based on the document's status as a draft*.
  - For example:
    - a draft safety evaluation that contains proprietary information (Exemption 4)
    - a draft document that contains classified information (Exemption 1)

FOIA Exemptions And Drafts (Cont.)

- Second, there is one FOIA exemption that can potentially apply to a draft document *because it is a draft*.
- Specifically: consider whether the draft document should be protected under the deliberative process privilege, which falls under **FOIA Exemption 5.**

FOIA Exemption 5

- FOIA Exemption 5, at 5 U.S.C. 552(b)(5), allows agencies to withhold "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."
- What does this mean?
- 1) Must be inter-agency or intra-agency record (i.e., not shared with parties outside the Executive Branch), *and*
- 2) Must be covered by a litigation privilege available to the government. These privileges include, most notably:
  - The attorney-client privilege
  - The attorney work-product privilege
  - The **deliberative process privilege**

Criteria For Applying Deliberative Process Privilege

1) Like anything under Exemption 5, the responsive record must be an **inter-agency or intra-agency** record, not shared outside the Executive Branch

2) Information must be **predecisional**

3) Information must be **deliberative**

4) Must **reasonably foresee harm** if information is released publicly

5) Record must be ***less than 25 years old*** as of date of request

6) Record must **not be expressly incorporated into final agency decision**

Inter/Intra-agency Requirement

- The deliberative process privilege is intended to protect the federal Executive Branch's ability to deliberate *internally* before making decisions.
- Sharing a draft document with parties outside the Executive Branch (e.g., applicants, licensees, vendors, trade associations, and potentially even states, local governments, or Indian Tribes) can therefore ***waive*** the privilege, making it unavailable in the future if the document is requested under FOIA.
- But sharing documents with other Executive Branch agencies (i.e., "inter-agency" sharing), or with persons or entities whose function is to advise the government (e.g., consultants retained by the government, federal advisory committees like ACRS) would **not** likely waive the privilege.

Predecisional Requirement

- The inter-agency or intra-agency record must contain "predecisional" information in order for that information to be withheld under the deliberative process privilege.
- The focus here is on timing.
- Generally speaking, information is "predecisional" if the record containing it predates some decision, or at least some potential decision, to which it relates.

Predecisional Requirement and Draft Documents

- Generally, a draft document will qualify as predecisional
- At minimum, a draft is predecisional relative to the final version of the document (whether the final is actual or merely hypothetical).
- For this purpose, "draft" is not referring to wikis or other "living documents," or to other documents that are intended for use as-is but may be revised in the future.

Deliberative Requirement

- **Key question**: does releasing this draft reveal anything about the agency's internal deliberations on the matter?

Deliberative Requirement and Draft Documents

- **Answer for drafts: Yes (usually)**.
- At minimum, a draft document reveals details—whether substantive, editorial, or both—about the agency's internal process for developing the document's final version (or for developing a hypothetical final version, if there isn't, or never will be, a final version).

Foreseeable Harm: General Rule Under FOIA

- **Foreseeable Harm Finding is a Statutory Requirement:** After 2016 amendments, FOIA now states that an agency may withhold information using a FOIA exemption only if:
  1. The agency reasonably foresees that disclosure would harm an interest protected by an exemption; or
  2. Disclosure is prohibited by law.
- **For Drafts: Must find foreseeable harm before withholding:** This is because withholding information under the deliberative process privilege is *discretionary* for agencies, not a legal mandate.

Foreseeable Harm: Types of Harm

- Typical types of harms that the deliberative process privilege is intended to protect against:
  - **Public confusion**
    - i.e., public may think draft indicates official agency position even if document does not yet look like the final version.
  - **Chilling effect on candor within the agency**
    - i.e., agency personnel may tend to self-censor when drafting documents or commenting/editing if they think their preliminary draft, comments, or edits will be released for public consumption → the concern is that this will lead to agencies making poorer, less well-considered decisions.
  - **Harm to the integrity of the agency's decision-making process**
    - This is the concern that revealing internal decision-making process details will preclude the final decision from speaking for itself.

Foreseeable Harm Statements

- **Required at NRC**: A foreseeable harm statement is a required step in the NRC's FOIA process when proposing to withhold information under the deliberative process privilege.
- **Conclusory statements do not suffice:** It is *not* enough in a foreseeable harm statement simply to state that releasing predecisional deliberative information is harmful or restate the harms listed on the previous slides.
  - As outlined in **Management Directive 3.4**, the NRC contemplates that predecisional information *could be released* in certain circumstances.
  - The **Commission** also makes many **notation vote SECY papers** publicly available, even though they are plainly predecisional and deliberative.
  - Thus, the agency's view is that releasing deliberative process information **is not *necessarily* improper**.
- Rather, the foreseeable harm statement must explain, **with at least some specificity**, why *the particular predecisional/deliberative document(s) in question* would foreseeably cause harm if released
  - Note: it is usually fine for a single harm statement to address an entire set of related documents, and it often requires only a paragraph or two.

Record Must Be Under 25 Years Old

- Protection under the deliberative process privilege via Exemption 5 is now, by statute, time-limited to 25 years, based on the age of the record relative to the date of the FOIA request.
- **This applies only to the deliberative process privilege**.

Record Must Not Be Expressly Adopted/Incorporated Into Final Decision

- Lastly, while this should be **rare for draft documents**, if a draft document were, for some reason, expressly adopted incorporated by reference into an official agency decision, then it loses any deliberative process privilege protection it might otherwise have enjoyed.

Duty to Release Reasonably Segregable Non-exempt Information

- **Must reasonably segregate and release non-exempt information**: Under FOIA, if a record contains exempt information, agencies are still required to release any "reasonably segregable" non-exempt information in the record. To do so, **redact** the exempt information.
- **Cannot withhold if no foreseeable harm:** Even if all information in a draft is predecisional and deliberative, only portions of the document whose release would foreseeably cause harm may be withheld.
- **Case-by-case assessment required:** Decisions on whether or how to reasonably segregate information in a draft document are generally case-by-case decisions: there is no magic, one-size-fits-all formula.
- **Is there a final version of the document?** Though the analysis is case-by-case, the existence or non-existence of a final version often is key.

No Final Version: Withhold Draft in Full??

- **Often, can withhold draft in full**: If there is no final version of the document yet, or if there will never be one (because the task was ultimately cancelled before the document was finalized), there are often strong reasons to withhold in full.
- **Why?**
  - If there is no final version, there may be no way to reliably determine, in the FOIA process, whether *anything* in the draft reflects:
    - the agency's official position on the matter discussed; or
    - the agency's official views on how to explain that position.
  - Moreover, the agency may ultimately decide (or, may have already decided) not to finalize a position on the matter at all.
- Thus, if there is no final version, withholding the draft in full is often the only way to prevent foreseeable harms of the sort the deliberative process privilege is designed to protect against.

But maybe not…

Nonetheless, there could be reasons to consider not withholding in full, even if there is no final. For example:

- **Discrete, purely factual discussions**: factual discussions in the draft that are set apart from other portions of the draft, are not controversial or in doubt, and required little editorial discretion to present, might not meaningfully reveal deliberations if released.
- **NRC has already said it publicly**: Portions of the draft might match publicly available agency statements in other NRC documents.
- **NRC has been public about its deliberations:** If the nature of the NRC's deliberations on the matter are already publicly known, release of the draft, whether in part or in full, may not reveal anything new.

These are not hard-and-fast rules, but they *may*, depending on the context, support a release, at least in part.

Final Version Exists: Release Draft in Part??

- If there is a final version, **consider whether to redact the differences between draft and final**: If this would avoid foreseeable harm, then it must be done.
- **What differences to redact**? Focus on:
  - Substantive differences;
  - Significant editorial differences (e.g., that substantially change how the substance is presented or described, or that significantly rearrange portions of the document);
  - Margin notes/comments.
- **Less important to redact**:
  - Typo fixes;
  - Routine or minor formatting changes.
- Note: if all differences are very minor: may be fine to release in full.

But maybe not…

- The redactions' **extent or location**, when viewed in light of the final, could still reveal significant deliberative information, such as:
  - How much, or how little, of the document was authored by the final agency decision-maker (as opposed to his/her subordinates)
  - What areas of the document were a focus of agency deliberations.
  - Whether agency staff proposed options (even of unknown content) that their superiors rejected before finalizing the document.
  - Whether a particular staff member's draft was well-received or not by supervisors/reviewers.
- Further, **some types of documents are routinely withheld in full, even if there is a final version**, to safeguard the integrity of the deliberative process (e.g., Licensing Board and Commission **adjudicatory decision drafts**).

Multiple Drafts: Do We Really Need to Process Them *All* Under FOIA?

- **Generally, yes**: If multiple drafts of a document are all "records" under FOIA, and all fall within the scope of the FOIA request, then the answer is yes, they must all be processed under FOIA as responsive documents.
- **Exception for personal records**: If a particular draft was not shared with other people, however, it may qualify as a "personal record," which would not be covered by FOIA.
- **For a series of related drafts**, it will often make sense to apply the same basic approach (i.e., what types of information to withhold, redact, and release) to each version. Plus, one harm statement would likely cover them all. These factors should speed up processing.
- **Verify that requester really wants them**. It may be worth discussing with the FOIA office whether the FOIA office should get clarification from the requester on whether he/she really wants all the drafts.

Final Takeaway: Withholding Drafts Often OK, but Not Automatic

- **It is usually fine to withhold drafts**: Generally, courts in FOIA lawsuits have been willing to uphold agency withholding of draft documents via the deliberative process privilege under Ex. 5.
- **But not automatic**: Nonetheless, courts have indicated that drafts are not *automatically* protected simply because they are drafts. Where agency reasoning is cursory or conclusory, court has ruled against the agency.
- Thus: **must still think through** the deliberative process privilege elements to ensure the draft is appropriate to protect, and whether protection should be full or only partial.

QUESTIONS?

Critical Electric Infrastructure Information

CEII

Who, What, When, Where of CEII

- The Fixing America's Surface Transportation (FAST) Act created a statutory category of information called critical electric infrastructure information or CEII. (Public Law 114-94, Sec 61003, 12/04/15; Sec 215A of Part II of the Federal Power Act, 16 U.S.C. 824o-1)

- The Federal Energy Regulatory Commission (FERC) was given the authority to designate as CEII both its own information and information of other agencies. (CEII is defined in 18 CFR § 388.113 - Critical Energy/Electric Infrastructure Information 12/21/16).

- "(1) Critical electric infrastructure information means information related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the [FERC] or other Federal agency other than classified national security information, that is designated as [CEII] by the [FERC] . . . pursuant to [the FAST Act]. Such term includes information that qualifies as critical energy infrastructure information under the [FERC's] regulations.

- (2) Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:
  - (i) Relates details about the production, generation, transportation, transmission, or distribution of energy;
  - (ii) Could be useful to a person in planning an attack on critical infrastructure;
  - (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
  - (iv) Does not simply give the general location of the critical infrastructure."

CEII and FOIA

- CEII is exempt from public disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3). Withholding under Exemption 3 is mandatory and non-discretionary.
- CEII should be withheld using Exemption 3 as well as any other applicable exemptions, such as Exemption 4 and/or Exemption 7F if applicable.
- Only FERC can formally designate NRC information as CEII. However, the FERC has encouraged other Federal agencies to take all necessary steps to protect information that may be CEII.
- Certain information that the NRC handles associated with critical infrastructure (e.g., nuclear power plants, dams, electric grid) could qualify as CEII.
- NRC-FERC MOU June 6, 2018

NRC-FERC-MOU

- Scope of NRC-FERC MOU ML18164A182
- General Responsibilities and Guidelines
- Identification and Labeling of CEII in the Custody of NRC
  - FERC's CEII regulations do not limit NRC's ability to take all steps to protect information that it considers to be CEII.
  - NRC staff is responsible for initially identifying and labeling CEII.
- Consultation with FERC's CEII Coordinator
  - The MOU sets forth a process for the NRC to request from FERC a supporting determination of the designation of material as CEII pursuant to Section 215A of Part II of the Federal Power Act.
  - If material that NRC staff considers CEII is requested under FOIA, NRC, through OCIO, will consult with FERC's CEII Coordinator to receive a FERC determination and designation that the material constitutes CEII.
- Protection and Handling of CEII
  - NRC will handle CEII information consistent with its procedures for handling other similar sensitive security material.

Labeling & Handling CEII

- This information requires specific protections.

- Label and handle the following information as CEII:
  - Security-related information (SRI) associated with critical infrastructure; or
  - Information associated with critical infrastructure that could reasonably be expected to endanger the life or physical safety of any individual, if released (typically information that qualifies under FOIA Exemption 7F).
  - Note: When information qualifies as both CEII and SRI, both markings should be used.

- Any NRC information that is potentially CEII or that has been formally designated by FERC as being CEII are to be marked "CEII -- DO NOT RELEASE." Information received from other agencies or external parties may already be marked as CEII, including "CEII," "CEII – Do Not Release," "Controlled Unclassified Information/CEII," or "Contains Critical Energy Infrastructure Information – DO NOT RELEASE." All CEII must be protected in accordance with the controls defined on the Sensitive Unclassified Non-Safeguards Information (SUNSI) Web page (see the link to the CEII Web page).

References

- PUBLIC LAW 114–94—DEC. 4, 2015, Fixing America's Surface Transportation Act. Section 61003, Critical Electric Infrastructure Security, 129 Stat. 1773-79. Section 215A of Part II of the Federal Power Act, 16 U.S.C. 824o-1.

- Federal Energy Regulatory Commission (FERC) promulgated rulemaking for 18 CFR 388.113 - Critical Energy/Electric Infrastructure Information (CEII) – December 21, 2016

- Memorandum of Understanding Between U.S. Nuclear Regulatory Commission ("NRC") and the Federal Energy Regulatory Commission ("FERC") Regarding the Treatment of Critical Energy/Electric Infrastructure Information ("CEII") ML18164A182

- SUNSI web page for CEII: http://drupal.nrc.gov/sunsi/34638

Questions?

OCIO FOIA Team
September 26, 2018 FOIA Seminar Evaluation Form

1) How did you find out about this event?

---

2) How useful to your work is the information you learned at this event?

☐ Extremely useful ☐ Useful ☐ Not very useful

---

3) Did this event meet your training expectations? ☐ Yes ☐ No

Comments:

---

4) Please rate the following for each of our topics (4=Excellent, 3=Very good, 2=Good, 1=Not very good):

<u>FOIA Overview and Processing Steps</u>

Usefulness of topic	☐ 1	☐ 2	☐ 3	☐ 4
Presentation	☐ 1	☐ 2	☐ 3	☐ 4
Handouts/Materials	☐ 1	☐ 2	☐ 3	☐ 4
Clarity of presentation	☐ 1	☐ 2	☐ 3	☐ 4

<u>Records</u>

Usefulness of topic	☐ 1	☐ 2	☐ 3	☐ 4
Presentation	☐ 1	☐ 2	☐ 3	☐ 4
Handouts/Materials	☐ 1	☐ 2	☐ 3	☐ 4
Clarity of presentation	☐ 1	☐ 2	☐ 3	☐ 4

<u>Draft Documents</u>

Usefulness of topic	☐ 1	☐ 2	☐ 3	☐ 4
Presentation	☐ 1	☐ 2	☐ 3	☐ 4
Handouts/Materials	☐ 1	☐ 2	☐ 3	☐ 4
Clarity of presentation	☐ 1	☐ 2	☐ 3	☐ 4

<u>CEII</u>

Usefulness of topic	☐ 1	☐ 2	☐ 3	☐ 4
Presentation	☐ 1	☐ 2	☐ 3	☐ 4
Handouts/Materials	☐ 1	☐ 2	☐ 3	☐ 4
Clarity of presentation	☐ 1	☐ 2	☐ 3	☐ 4

---

5) Your office: _____ Name & contact information (optional):

_____

6) Comments:

_____

_____

Thank you for your participation and feedback from our agency-wide training today. Please fill out and drop off at the back table of the Auditorium before you leave today, or mail to the FOIA Team at Mail Stop TWFN-8 D22M.

_____

Personally Identifiable Information and Privacy Act Responsibilities Awareness Course

Introduction

- This training is designed to ensure that NRC staff understand their responsibilities under the Personally Identifiable Information (PII) policy and Privacy Act of 1974.
- In accordance with the Office of Management and Budget (OMB) memorandum (M-17-12), "Preparing for and Responding to a Breach of Personally Identifiable Information," dated January 2, 2017, Federal agencies are required to ensure that all individuals are:
  - Aware of the responsibilities relative to protecting PII
  - Aware of the consequences and accountability for violation of these responsibilities
  - Acknowledge this understanding at least annually

Objectives

By the conclusion of this training, you will be able to:

- Identify the privacy responsibilities of Federal employees.
- Identify the appropriate use of information relative to the protection of information.
- Identify examples of information that might be considered PII.

What is PII?

PII is information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual.

PII is a person's name, in combination with any of the information listed on the right.

- Mother's maiden name
- Driver's license number
- Bank account information
- Credit card information
- Relatives' names
- Postal address
- Personal e-mail address
- Home or cellular telephone number
- Personal characteristics
- Social security number (SSN)
- Date or place of birth
- Or other information that would make the individual's personal identity easily traceable and usable

The Privacy Act

- The Privacy Act addresses a group of any records under the control of any agency from which information is **retrieved by the name of the individual or by some identifying number**, symbol, or other identifying information particularly assigned to the individual.

- The Privacy Act is designed to protect the individual's privacy from unwarranted invasion; to make sure that personal information in possession of Federal agencies is properly used; and to prevent any potential misuse of personal information in the possession of the Federal Government.

- A "system of records" is defined by the Privacy Act as a collection of records about an "individual from which information is **retrieved by name or personal identifier**," and, importantly, an "individual," is defined by the Act to be a citizen of the United States or a Legal Permanent Resident.

Is PII Protected under the Privacy Act?

Only PII that is included in a Privacy Act system of records will be protected by the provisions of the Privacy Act.

PII that is contained in documents, files, or databases not part of a Privacy Act system of records will not receive the legal protection of the Privacy Act, but you must still treat it in accordance with National Archives and Records Administration direction and applicable NRC policy for handling PII.

Personal Information not Covered by Privacy Laws

Employee information that is considered to be on public record as well as information that is releasable under the Freedom of Information Act (FOIA).

- Public record information includes basic employee information such as name, grade, salary, title, and duty station, and is generally releasable to the public.
- FOIA information that may be released to a requester under FOIA includes the following:
  - Information relating to qualifications for Federal employment
  - Position descriptions, critical elements, and performance standards
  - Postgraduate or technical training relating to the current profession
  - Earlier employment experience in a State or Federal Government position
  - Earlier employment experience (but not salary) in the private sector where related to current duties
  - Membership in professional groups
  - Awards, honors, and letters of commendation from professional associations and colleges

What is not PII?

Since personal identity is distinct from an individual's professional identity, the NRC does not treat the following information as PII:

- An individual's name
- An individual's title
- Work telephone number
- Official work location/address
- Work e-mail address

Is all PII Protected?

No, the NRC does not require the protection of the following PII:

- **Adjudicatory Filings, Documents Associated with Agency Rulemakings, and Correspondence Received from the Public on Regulatory Matters** - Home addresses, home phone numbers, or home e-mail addresses that individuals choose to include in these submissions are not considered PII because they are voluntarily submitted as part of a public process.

- **An NRC Employee's Name, Title, Work Telephone Number, Official Work Address, and Work E-Mail Address** - The NRC does not consider these to be PII since they are not personal information subject to misuse and reflect the employee's professional identity rather than his or her private information.

Exceptions from the General Provisions of the NRC PII Policy

- **General Exception: NRC Emergency Contact Listings/Duty Rosters** – Those with an official need-to-know may keep employee emergency contact lists of names, home and cellular phone numbers, and home e-mail addresses, in paper form or stored in personal electronic devices, outside of NRC-controlled space.

- **Specific Exceptions** – Office directors, regional administrators, and their designees may issue specific exceptions; however, the exceptions must be in writing and describe why unredacted documents are necessary and how the documents will be protected while outside NRC-controlled space. These specific exceptions shall be granted infrequently and a copy of the written exception must be provided to the Chief Information Officer (CIO).

- **Personal Exception** – Individuals may control the release, transport, and transmission of their own PII in conducting personal business or as necessary for agency use, such as for payroll or travel records. Using unencrypted electronic or voice communications or carrying unredacted hard copies of one's own PII represents a degree of risk for the loss of that information.

Why Do You Need to Know about Privacy and PII?

- It is information about individuals that the Federal Government collects, maintains, distributes, and destroys. It includes information about you.
- You must take precautions when handling PII in the performance of your job.
- The loss of, or unauthorized access to, PII can result in:
  - Substantial harm, embarrassment, and inconvenience to individuals, as well as our agency
  - Identity theft

What You Need to Know about Privacy and FOIA

- FOIA provides the public the right to request access to records from any Federal agency.
- Requests for records under both the FOIA and Privacy Act often contain sensitive information, including PII. However the records need to be provided in a clean, transparent version to the Office of the Chief Information Officer, Governance & Enterprise Management Services Division, Information Services Branch (OCIO/GEMS/ISB), in order for the FOIA staff to process. The FOIA staff have a **need to know** and will ensure the recommended portions of information to be withheld will fall within the scope of either a FOIA exemption or Privacy Act exemption.

What You Need to Know about Privacy and FOIA (continued)

Any person can request agency records under 5 U.S.C. § 552, the "Freedom of Information Act" (FOIA)

The Privacy Act (5 U.S.C. § 552a) grants individuals an increased right of access to records about them

- If a person makes a FOIA request encompassing records about **another person** (3rd party request) which are included in a Privacy Act System of Records, and there is no applicable **FOIA** exemption which would permit withholding, the records must be released
  - If there is an applicable FOIA exemption, the records should be withheld
- If a person makes a FOIA request encompassing records about **themselves** (1st party request) which are included in a Privacy Act System of Records, the request is treated as **both** a FOIA request and a Privacy Act request, and the records can be withheld **only** if there is applicable exemption under **both** statutes that permits withholding

What Information is Not Releasable Under FOIA?

The NRC may withhold information in a FOIA request if disclosure would result in an unwarranted invasion of personal privacy. In general, the NRC withholds the following information:

- Age, marital status, race, home address, home phone number, and social security number
- Medical records
- Performance appraisals
- Employment history that does not relate to the current job
- Allegations of misconduct and arrests, complaints, grievances, and performance-based actions
- Payroll deductions

Do Not Collect or Maintain PII

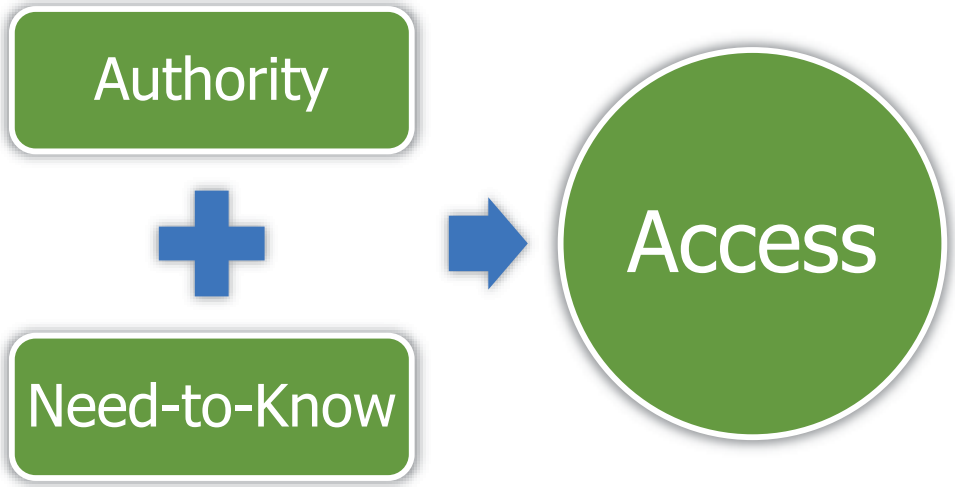
Do not collect or maintain PII unless you are authorized to do so as part of your official duties. Even then, you should only collect and retain PII that is relevant and necessary for NRC functions or responsibilities.

Use Authorized System of Records

Ensure that information retrieved by an individual's name or other personal identifier is maintained in an authorized Privacy Act system of records for which a system notice has been published in the *Federal Register*.

Verify Need-to-Know

Only disseminate PII to those NRC employees who have a need-to-know the information to perform their official duties, not a want-to-know.



Do Not Disclose PII

Do not disclose PII to anyone unless the disclosure is authorized for the purpose of conducting official business. This does not prohibit you from disclosing your own PII.

All NRC Forms and Surveys Must be Reviewed for PII

- All NRC forms and surveys must be reviewed by the Privacy Team in OCIO/GEMS/ISB to see if they ask for PII.
- The Privacy Team determines if the form or survey will need to have a Privacy Act Statement.
- Forms or surveys may not be used to collect information until the Privacy Team has reviewed them.
- Submit NRC forms and surveys for review:
  - Forms: Forms.Resource@nrc.gov
  - Surveys: Privacy.Resource@nrc.gov

Protect the Information

Maintain PII in a manner that will prevent inadvertent or unauthorized disclosures.

- Do not leave PII in open view of others, either on your desk or computer screen.
- Use an opaque envelope when transmitting PII through the mail.
- Secure paper records in a locked file drawer and electronic records in a password protected or restricted access file.
- Do not place or store PII on a shared network drive unless access controls are applied.
- Encrypt PII information being sent, via email, outside the Agency.
  - For instructions on encrypting emails, see http://drupal.nrc.gov/ocio/25726.

Storing PII on Shared Drives

- Contact the CSC Help Desk to create a secure restricted location to store PII information on Shared Drives.
- You must **NOT** store PII on shared access computer drives ("shared drives") unless access is restricted to those with a need to know by permissions settings or passwords.
- Verify access has been restricted properly.
- Remove or delete PII information when no longer needed
- If only you need access for your work, use your P Drive, this would be the wiser, more secure option.

NOTE: Most NRC users do not have the level of permission to restrict access

Storing PII on SharePoint Sites

- Contact your SharePoint Administrator to create a secure restricted location in SharePoint to store PII information.
- Do **NOT** post PII on SharePoint sites that can be accessed by individuals who do not have a need to know.
- PII on SharePoint sites **must** be restricted access only.
- Verify access has been restricted properly.
- Remove or delete PII information when no longer needed.

NOTE: Only SharePoint Administrators have the level of permissions to restrict access.

Transmitting PII

- Do not email or otherwise transmit PII that is included in a Privacy Act system or records outside the agency unless it is an expressly permitted disclosure under the Privacy Act (for example, a "routine use" published in the NRC's System of records notice).
- Information that is not included in a Privacy Act system or records but nonetheless still constitutes PII may not be sent outside the agency except where sent to an authorized recipient for the purpose of conducting official agency business.
- Only NRC email accounts can be used to send or receive e-mails when conducting official Agency business.
- E-mailing PII information outside the Agency **must** be **encrypted**.
- E-mailing PII to those with a need-to-know within the NRC local area network/wide area network is acceptable, including to and from electronic devices interacting within the NRC's e-mail system.
- Do not remove paper documents that contain PII of individuals, other than yourself, from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted. This does not apply to emergency contact information.
- Do not remove electronic PII from NRC-controlled space on mobile information technology (IT) devices, such as CDs, DVDs, or thumb drives unless all PII is **encrypted**.

Rules of Behavior for Authorized Computer Use

When using or accessing electronic PII, follow the NRC Agencywide Rules of Behavior for Authorized Computer Use.

Properly Destroy and Dispose of PII

- Properly destroy and dispose of PII that is no longer required.
- Do not place in regular trash or recycle bins.
- Before destruction, refer to the NRC records disposition schedules for applicable retention schedules.

Social Security Numbers

OMB M-17-12 and the Office of Personnel Management's memorandum dated June 18, 2007, require agencies to reduce the unnecessary use of SSNs.

- Eliminate the unnecessary collection or retention of SSNs.
- Eliminate the unnecessary use of SSNs as an identifier.
- Eliminate the unnecessary printing and displaying of SSNs on forms, reports, and computer display screens.
- Restrict access to SSNs only to those individuals whose official duty requires such access.

Violations

In accordance with the existing authority, the NRC may impose progressive disciplinary measures on employees for infractions of the agency's PII policy.

Violations involving security controls, unauthorized disclosure, unauthorized access, reporting requirements, and supervision may constitute a basis for a disciplinary action, including reprimand, suspension, removal, or other actions consistent with applicable law and policy.

In addition, appropriate legal action may be pursued for breaches of NRC PII caused by non-NRC employees, such as NRC contractors.

Types of Violations

Security Controls Violation

Failure of the responsible employee to implement and maintain applicable PII security controls of which the employee is aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

Unauthorized Disclosure Violation

Deliberate, unauthorized disclosure of PII to others. Infractions involving Privacy Act violations (willful disclosure of Privacy Act information to unauthorized recipient(s)) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

Unauthorized Access Violation

Deliberate, unauthorized access to or solicitation of PII. Infractions involving Privacy Act violations (requests for access to Privacy Act information under false pretenses) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

Reporting Requirements Violation

Failure to report any known or suspected loss of control or unauthorized disclosure of PII.

Supervision and Training Violation

Failure, as a manager, to adequately instruct, train, or supervise employees in their responsibilities.

Report Suspected or Confirmed Inadvertent Breaches

Use step 1 or 2 below as applicable:

1. Any release of PII where IT equipment/system is involved must be reported immediately to OCIO's Computer Security Incident Response Team (CSIRT) at CSIRT@nrc.gov or 301-415-6666.

2. Situations involving the improper handling or storage (no IT equipment/system involved) of PII must be reported immediately to the Office of Administration, Division of Facilities and Security (ADM/DFS) or the Duty Officer at ADM/DFS: DFS_RPT@nrc.gov or 301-415-6885. After hours, contact the Duty Officer through the Central Alarm Station: 301-415-2056 or 301-415-2200.

Report Suspected or Confirmed Deliberate Breaches

In addition to the steps for an inadvertent release, any potentially deliberate breach of PII requires immediate notification to the Office of the Inspector General (OIG) at 301-415-5930 or 301-415-5925, or the OIG Hotline at 800-233-3497.

Any other notifications or actions must be approved by the OIG under these circumstances as any action may impede their investigation.

Summary

In this course, you have learned how to:

- Identify the privacy responsibilities of Federal employees.
- Identify the appropriate use of information relative to the protection of information.
- Identify examples of information that might be considered PII.

Thank you.

You have completed this training.

You may close this window.