

## How to Respond to a Freedom of Information Act (FOIA) Request

What is FOIA?

The Freedom of Information Act (FOIA) is a law that gives any person the right to request access to records in the possession of or under the control of a Federal agency. An agency must provide access to those records unless it is exempted from disclosure by one of the nine exemptions (seven are regularly used by the U.S. Nuclear Regulatory Commission (NRC)) or three special law enforcement and national security exclusions in the act.

Who can make a FOIA request?

Almost any person can make a FOIA request including:

- individuals (regardless of their citizenship)
- corporations
- associations
- State and local governments
- foreign governments

Which records are subject to FOIA?

FOIA applies to all “agency records.” Agency records are any records created or obtained by an agency that are under the control of the agency at the time of a request. These include:

- (1) paper documents (including papers, maps, charts, photographs, and microfiche)
- (2) e-mails
- (3) other electronic records
- (4) audiovisual material (including sound and video recordings)

“Personal records” of an employee that are not under the control of the agency are not considered agency records.

### Steps to Follow When You Receive a FOIA Request

#### **1. Make Sure You Clearly Understand Which Records Are Being Requested**

The FOIA specialist will make every effort to clarify the scope of the request before forwarding the request to the respective office FOIA coordinators. If a request is overly broad in scope, unclear, would generate a voluminous amount of records, or would impose a burdensome search, please contact your FOIA coordinator to let him or her know. If you believe it would be helpful to participate in a conference call with the requester about the request, ask your office FOIA coordinator to contact the FOIA specialist assigned the request to facilitate a conference call with the requester. During this call, you may ask questions or offer suggestions to further define the scope of the request.

Note: Do not make any contact with the requester on your own.

## **2. Determine If You Are Likely To Have the Requested Records**

Based on your knowledge of the subject matter of the request, you should determine if you have records responsive to the request. To be considered an adequate search, you are only required to search in places that you reasonably expect to contain responsive records.

No records that are potentially responsive to a FOIA request may be destroyed after the agency's receipt of the FOIA request.

Only agency records that are in existence on the date a request was received should be provided in response to a FOIA request. This includes readily reproducible electronically-stored information.

Do not create a record to respond to a request; however, extracting information from an existing database (or list) does not count as creating a new record.

To determine whether personal records, such as notes taken during a training class or journals, personal correspondences, or other personal notes not used during the course of transacting Government business, please refer to NRC Form 510, Personal Records Checklist (see Exhibit A). Give the completed NRC Form 510 to your office FOIA coordinator.

If you believe responsive records may be located in other offices, including with people who may have been previously involved in the subject matter or members of a team or project, provide that information to your office FOIA coordinator promptly. The FOIA specialist will contact the additional office(s) and request a search for records.

## **3. Provide a Fee Estimate, If Required**

Within 4 working days of your office's receipt of the request, you may be required to provide to the FOIA specialist a fee estimate, which may include the amount of time expected to be required to search for and review responsive records, including the estimated number of pages expected to be released to the requester. Whether your office will need to provide a fee estimate depends on the fee category of the requester and whether the requester has been granted a fee waiver (see Exhibit B, Fee Categories). Include the following applicable information with your estimate:

- (5) Search—All time spent locating records responsive to a FOIA request. This includes time spent locating records in file cabinets, file folders, ADAMS, and other databases, e-mails, and NRC computer hard drives (desktop and network).
- (6) Review—Review time spent by the subject matter expert examining records retrieved in response to a request to determine whether they are exempt from disclosure in whole or in part. Review time also includes the time devoted to examining records to determine which FOIA exemptions, if any, are applicable and identifying records, or portions thereof, that should be disclosed.

- (7) Duplication—Estimate the number of pages likely to be released to the requester. This does not include staff hours used to copy records.

#### **4. Process Expedited Requests First**

Your office FOIA coordinator will inform you if a request has been granted expedited processing. If a request has been granted expedited processing, you should process the expedited FOIA requests ahead of any other FOIA requests previously assigned to you. Contact your office FOIA coordinator for more specific directions, if needed.

#### **5. Search for Records Responsive to the Request**

- Your office FOIA coordinator will tell you when to begin your search.
- Conduct a search of paper and electronic files that you reasonably expect contain responsive records (e.g., file cabinets, e-mails, ADAMS, SharePoint, other databases, microfiche, photographs, audiotapes, and videotapes). Even if older records are stored, at offsite records centers, you should consider whether they are responsive to a request and take the necessary steps to arrange for their retrieval.
- If a record is publicly available, provide the ADAMS accession number or the Web address where the record is located.
- If a record has been physically and legally transferred to the National Archives and Records Administration (NARA), and no copies are in the custody of the NRC, notify your FOIA coordinator that the records have been transferred.

#### **6. Provide Your Recommendation On the Release of Information**

After you have searched and located records, you should review them and provide your disclosure recommendations by:

- Marking portions of the records considered exempt with the applicable exemption (any marking may be done using Adobe, see Exhibit C) or
- By describing the nature or items of information considered exempt with the applicable exemption. (This can be completed directly on NRC Form 511, Program Office Response to a FOIA Request). (see Exhibit D)

For guidance on how to process investigative and allegation-related records (see Exhibit E, FOIA Processing Guidance for Investigation and Allegation-Related Materials).

NOTE: Sensitive unclassified non-safeguards information (SUNSI) and controlled unclassified information (CUI) can only be withheld if there is an applicable exemption.

Sometimes while reviewing records you will find information that is outside the scope of the request. Do not provide entire pages of records that are outside the scope of the request. If outside-of-scope information is intertwined with information that is responsive to the request, identify portions of the record that are outside the scope of requested information. You do not need to consider whether any FOIA exemption should be applied to outside-of-scope information (see example of Outside the Scope Markings, Exhibit F)

## **7. Organize the Records Responsive to Request and Submit Them to Your Office FOIA Coordinator**

In organizing the responsive records, provide print-outs and listings of the records already publicly available in ADAMS or elsewhere on <http://www.nrc.gov>, as well as records to be moved from the nonpublic ADAMS site to the public ADAMS site. For all other responsive records, clearly identify the following:

- information and records recommended for discretionary release
- records to be referred to another office (but you should include your own disclosure recommendations as well)
- records to be referred to another Federal agency (i.e., documents that belong to another Federal entity)
- records to be referred to a licensee (or other business submitter)

Records submitted to the FOIA office should not be grouped based on their disclosure recommendation (e.g., records must not be separated into “release in part,” “released in full,” “licensee records,” etc.)

- If applicable, complete NRC Form 496, Report of Staff Resources for Processing FOIA Requests (see Exhibit G). Include in your response the actual search time and review time spent on processing the request.
- In situations in which the Secretary of the Commission, Office of the General Counsel, or the Office of the Inspector General (OIG), NRC exercises its authority to retain records responsive to a FOIA request, it is required to provide the FOIA specialist with an appendix. The appendix must include the date of the record, a description, and the page count for each record.

Note: An email or memorandum that has one or more attachments, and a letter that has one or more enclosures, are considered a single record. Do not separate attachments/enclosures from the email/memorandum/letter.

## 8. Submit Response Package to the FOIA Specialist

You are required to provide your office FOIA coordinator your response package within the timeframe specified by your office. Within 10 working days of your office's receipt of the request, your office's response—consisting of responsive redacted records—is due to the assigned FOIA specialist. If you cannot respond within your office's timeframe, you should obtain management approval and inform your office FOIA coordinator as soon as possible when you expect to provide a complete response. You must also provide a foreseeable harm statement when Exemptions 2 or 5 apply. Because the FOIA office tracks all discretionary releases at the end of the reporting year as part of the annual FOIA report and the Chief FOIA Officer's report, in the event that a discretionary release is being made, cite the exemption that would have been applicable (either Exemption 2 or Exemption 5) and clarify that your release recommendation is discretionary.

### Description of the FOIA Exemptions Regularly Used by the NRC

#### □□ Exemption 1

Protects national security information that is properly classified under the procedural and substantive requirements of the Executive order on classification, in effect when the classification was made. . Proper classification markings are: Confidential, Secret, and Top Secret.

Criteria:

- Information meeting standards set forth by Executive order to be kept secret in the interest of national defense or foreign policy, including information about Federal Government programs to safeguard nuclear materials or facilities, vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services related to national security, including defense against transnational terrorism. If unauthorized disclosure of information could be expected to cause damage to national security; that original classification authority should be able to identify or describe.
- Information properly classified under Executive order by designated classification authorities applying approved classification guidance to specific documents and marked accordingly.
- Information that is not in the public domain.
- Mosaic or compilation approach is acceptable when compiled information reveals additional association that meets classification standards in the Executive order and is not otherwise revealed in individual items of information (see mosaic at the end of the Exemption 9).

Examples of classified information:

- Information related to security of fuel cycle facilities possessing strategic quantities of special nuclear material.
- Information about security systems (e.g., guards, alarms, duress codes) of certain facilities or activities that would aid an adversary in attacking a facility or mode of transportation.
- Foreign government information provided with an understanding or agreement that information is considered classified or confidential by the supplying foreign government.

### **Exemption 2**

Protects information that is related solely to the internal personnel rules and practices of an agency. This exemption is limited only to issues of employee relations and human resources, such as hiring and firing, work rules and discipline, and compensation and benefits.

**(A foreseeable harm statement must be provided, if applied).**

Criteria:

- internal information
- practices and rules only affecting agency personnel; not applicable to the public and not mission-related
- human resources or employee relations information, rules, or guides
- no genuine and significant public interest

Examples of information that may qualify for Exemption 2 protection:

- crediting plans (if the agency expects to use the plans again in the future)
- employee emergency exit procedures, shelter-in-place plans, and so on
- personnel security practices
- procedures for employee performance evaluations
- internal procedures for responding to employment-related complaints
- Internal publications
- employee bulletins or announcements
- leave practices

- parking rules

### **Exemption 3**

Protects information that has been specifically exempted from disclosure by other Federal statutes. Statutes may fall under this exemption if they:

- (1) Establish an absolute prohibition on disclosure; or
- (2) Establish particular criteria for withholding or refers to particular types of information that must be withheld.

Criteria:

- Nondisclosure mandate must be contained in a Federal statute.
- General disclosure of information must be prohibited on the face of the statute or by establishing particular criteria or reference to specific types of information to determine which information is within the scope of the statute's prohibition.
- Restricted data, under Section 11y of the Atomic Energy Act (AEA), must encompass information related to design, manufacture, or use of atomic weapons or the production or use of special nuclear material.
- Safeguards information, under Section 147 of the AEA, should encompass information prescribed by regulation in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.2, "Definitions," and 73.21, "Protection of Safeguards Information: Performance Requirements" (or by order). These specifically identify the following detailed information for a licensee or applicant:
  - security measures for the physical protection of special nuclear material
  - security measures for the physical protection and location of certain plant equipment vital to the safety of a facility possessing nuclear materials subject to NRC jurisdiction
  - design features of the physical protection system
  - operational procedures for the security organization
  - improvements or upgrades to the security system
  - vulnerabilities or weaknesses in the security measures or systems described above that have not yet been corrected

- other information as the Commission may designate by order or regulation upon making the necessary findings under Section 147. (Note: description augmented subject to the Commission issuing a final rule amending 10 CFR Part 73.)
- Contractor proposals, under Section 253(m) of the National Defense Authorization Act for Fiscal Year 1997, submitted by a contractor in response to the requirements of a solicitation for competitive proposal that are not set forth or incorporated by reference in the contract.

Examples of information that are prohibited under Exemption 3:

- Restricted Data—includes technological details of uranium enrichment technologies (e.g., diffusion, centrifuge, laser-based enrichment) and technologies in certain defense systems, such as the Navy nuclear program.
- Safeguards Information—includes details from a licensee’s physical security plan, such as the number of guards and specific location of security equipment.
- Contractor proposals—those submitted by unsuccessful offerors in response to a solicitation.
- Contractor proposals—those submitted by the successful offeror in response to a solicitation not set forth or incorporated by reference in the contract.

Examples of information outside mandatory prohibition against disclosure include the following:

- security measures for physical protection of facility in plain sight of public
- physical protection design details readily available to the public
- contractor proposals set forth or incorporated by reference in a contract

#### **Exemption 4**

Prevents disclosure of trade secrets, as well as commercial or financial information received from a person that is considered privileged or confidential (often referred to as “proprietary information”):

Criteria for information other than trade secrets to qualify for protection under Exemption 4:

- Information must originate outside the Federal Government.
- Information must be commercial or financial
- Information must be privileged or “confidential” within the meaning of the exemption.

- If provided to the agency voluntarily, it would not be customarily released to the public by the submitter of the information
- If submission of the information was required, disclosure would likely impair the Government's ability to obtain necessary information in the future, could cause substantial competitive harm to the person who provided it, or could impair Government interests of compliance or program effectiveness.

Examples of information that may qualify for Exemption 4 protection include:

- product manufacturing and design information
- nonpublic financial statements
- settlement agreements
- customer lists
- information submitted in confidence by a foreign source
- detailed plant security information, such as a licensee control and accounting procedures for safeguarding licensed nuclear material or detailed measures for the physical security of a licensed facility, if the information could facilitate attempts at sabotage, diversion of nuclear material, or other attacks detrimental to public health and safety
- information generated outside the Government revealing vulnerabilities of nuclear facilities or materials to theft or sabotage
- certain facility drawing details showing specific locations of equipment or materials within buildings
- private sector information that, if disclosed, could reasonably jeopardize a Government security program's effectiveness

Examples of information that would not qualify for Exemption 4 protection:

- general information about a product's physical or performance characteristics or product formula
- financial information in a company's prospectus or annual report
- general descriptions of safety-related systems in nuclear power plants, particularly if available in open-source literature or on Web sites accessible to the public
- general information about workings of a nuclear power plant, such as that provided in licensing documents

- low-resolution drawings of plant site and adjacent areas

For proprietary information submitted by a licensee or other business submitter, provide a copy of the affidavit supporting its request that the information be protected from public disclosure and the NRC's determination letter sent to the company.

In the absence of a supporting affidavit, provide records and submitter contact information to your office FOIA coordinator so that the coordinator can provide it to the FOIA specialist, who will initiate contact with the licensee or business submitter.

### **Exemption 5**

Protects inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency. The three privileges most often invoked under Exemption 5 are the deliberative privilege, the attorney–client privilege, and the attorney work product privilege. **(A foreseeable harm statement must be provided, if applied to claim the deliberative process privilege.)**

Criteria include the following:

- Communication that is internal to the Federal Government (within the agency or among Government agencies)
- Reasonably segregated material not covered by the exemption must be disclosed (i.e., an entire record is not automatically exempted)
- Deliberative process privilege, which covers material reflecting predecisional analysis, recommendation, or opinion on matters leading to final decision but not purely factual information, unless disclosure would tend to reveal the nature of protected deliberations
- Attorney–client privilege, which covers confidential facts related by a client to an attorney and legal opinions and communications between them concerning the consultation
- Attorney work product privilege, which covers material prepared in contemplation of litigation, including administrative proceedings
- Requests, such as a draft containing preliminary recommendations. Such records might be eligible for withholding under Exemption 5 because they contain analysis and recommendations that constitute part of a deliberative process but are not the end of the agency's review. In such cases, the age, content, and character of such a draft should be reviewed to determine if the agency reasonably foresees that this disclosure would harm an interest protected by Exemption 5.

Examples of privileged material that may fall under Exemption 5:

- portions of briefing papers or drafts of security-related or non-security-related documents

- security or non-security-related policy analyses and recommendations produced by agency employees
- analysis of an agency's litigative risk in security-related or non-security-related hearings
- description of an agency's legal strategy in proceeding on security-related or non-security-related matters.
- records received from outside an agency only if they are created by external experts working as if they were NRC employees

Examples of material outside privilege include:

- final agency decisions that expressly incorporate pre-decisional analysis
- after-the-fact descriptions or explanations of agency policy or decision
- segregable facts from documents otherwise subject to deliberative process privilege

### **Exemption 6**

Protects information in personnel and medical files and similar files, which, if disclosed, would constitute a clearly unwarranted invasion of personal privacy. Living individuals have a privacy interest in not having agencies disseminate personal information about them.

Criteria include the following:

- Information must be about an individual.
- Decisions should balance public interest and the individual's privacy interest.
- Information should be located in a file other than an allegation or investigative file (also see Exemption 7(C) below).
- Information is about or has an impact on a living person.

Examples of information that may qualify for Exemption 6 protection include:

- social security numbers
- home address and telephone numbers
- personal cellular and pager numbers
- personal e-mail addresses

- dates of birth
- marital status
- non-job-related interests
- medical and financial information
- religious affiliation or references to religious activities
- performance and disciplinary information

Examples of information that generally do not qualify for Exemption 6 protection include:

- information on deceased individuals, except in rare cases where a living person would be offended by the details
- responses are to a Federal vacancy announcement and include rating factors for the selected individual
- individual is covered by a Federal employee position description
- individual has Federal employee performance elements and standards are covered by Federal employee grade and salary information

### **Exemption 7**

Protects information compiled for a law enforcement purpose including information compiled to prevent circumvention of the law. Protects information if disclosure causes one or more of six types of law enforcement harm.

Criteria include the following:

- Information compiled for law enforcement purposes would jeopardize statutory protections, including information that, if disclosed, could reasonably be expected to interfere with enforcement proceeding (Exemption 7(A)), right to fair trial; (Exemption 7(B)), right to be free from unwarranted invasions of personal privacy; (Exemption 7(C)), protection of identity of confidential source; (Exemption 7(D)); protection of law enforcement techniques and procedures, or guidelines where disclosure could risk circumvention of law; (Exemption 7(E)); disclosure could reasonably be expected to endanger life or physical security of any individual (Exemption 7(F)).

NOTE: The Exemption 7 subparts are applicable to investigative records and non-investigatory records compiled for law enforcement purposes, including the prevention of future illegal acts under the agency's mandate to protect people and property. The law enforcement purpose need not be the only reason for compiling the records.

Examples of information that may qualifying law enforcement information include:

- Investigations focused on misconduct or potentially unlawful activity.
- Security-related or non-security-related information developed by the Office of Investigations used to determine whether enforcement action should be taken against a licensee.
- Security and safety information in reports of inspections conducted to determine compliance with regulatory requirements when violation of those requirements could endanger the life or physical security of any individual.
- Security or safety information compiled for the purpose of protecting people and the environment when disclosure of the information could endanger the life or physical security of any individual.
- Allegations of security-related or non-security-related violations received from outside the agency and related analyses prepared by or for the Office of Enforcement to determine if sanctions should be imposed against the violator.

Examples of non-qualifying law enforcement information include:

- Routine security and non-security inspection reports.

Examples of information that may qualify for Exemption 7(A) protection include:

- Information that could reasonably be expected to interfere with an open allegation.
- Information that could reasonably be expected to interfere with an open investigation in the Office of Investigations.
- Information that could reasonably be expected to interfere with an open investigation in the OIG information that could reasonably be expected to interfere with an ongoing enforcement action

Note: Records withheld under Exemption 7A must be retained for 6 years from the date of the agency's final response.

Examples of information that would not qualify for Exemption 7(A) protection include:

- allegation, investigatory, or enforcement information on closed matters

Exclusions include the following:

Whenever a request is made that involves access to records subject to Exemption 7(A), the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of the FOIA when the following apply:

- The investigation or proceeding involves a possible violation of criminal law; and there is reason to believe that: the subject of the investigation or proceeding is not aware of its pendency, or disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings.

Examples of information that may qualify for Exemption 7(B) protection include:

- rarely invoked, an application of Exemption 7(A) normally would protect defendants' interests just as well, as would Exemption 5, outside the context of law enforcement purposes
- records or information compiled for law enforcement purposes, the disclosure of which would deprive a person of a right to a fair trial or an impartial adjudication

Examples of information that would not qualify for Exemption 7(B) protection include:

- records or information compiled for law enforcement purposes the disclosure of which could interfere with the fairness of the proceedings, but no trial or adjudication is pending or truly imminent

Examples of information that may qualify for Exemption 7(C) protection include:

- personal information in closed allegation, investigatory, or enforcement files (see Exemption 6 for specific examples).

Examples of information that would not qualify for Exemption 7(C) protection:

- personal information located in files other than an allegation or investigative file.

Examples of information that may qualify for Exemption 7(D) protection:

- information that could reasonably be expected to disclose the identity of a confidential source
- information provided by a confidential source, in certain situations, whether or not the information itself could identify the source

Examples of information that would not qualify for Exemption 7(D) protection include:

- information related to individuals who have not been granted confidentiality (no balancing of public interest)

Examples of information that may qualify for Exemption 7(E) protection include:

- technique information is not well known to the public

- meets law enforcement guidelines (no legitimate public interest in the disclosure of information that would assist in the evasion of law or detection)

Examples of information that would not qualify for Exemption 7(E) protection include:

- routine techniques

Examples of information that may qualify for Exemption 7(F) protection:

- records or information compiled for law enforcement purposes that, if disclosed, could endanger the life or physical safety of an individual or individuals (for instance, an individual (or group of individuals) who has been threatened in the past)

### **Exemption 8**

Applies to financial institutions (This exemption not used by the NRC).

Statutory description: Matters that are contained in or related to examination, operating, or condition reports prepared by, or on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.

### **Exemption 9**

Applies to wells (This exemption not used by the NRC).

Statutory description: Geological and geophysical information and data, including maps, concerning wells

### **Glomar Response:**

- The term “glomar response” or “glomar denial” refers to a “neither confirm nor deny” response to a FOIA request. As an example, the NRC provides a glomar response in situations in which a requester seeks investigative information on a named individual(s) when a response as to whether or not a person is or is not mentioned in an investigative record may have a stigmatizing connotation.

### **Mosaic (or Compilation) Theory**

- Under FOIA, an agency is required to disclose any information that does not fall within one of the FOIA exemptions. However, some information, while seemingly suitable for public release on its own, can be extremely harmful when grouped with other information (that is either also responsive to the request or has been released publicly, or to the requester). To provide protection from public disclosure of information that merits protection because of the context in which it is presented, the courts have sanctioned the use of the “mosaic” or “compilation” theory, which is explicitly recognized in the classification in Executive Order 13526 that sets forth the standards for classifying national security information.
- Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the following: (1) meets the standards for classification under this order, and (2) is not otherwise revealed in the individual items of information.

“Compilation” means an aggregation of pre-existing unclassified items of information (Section 1.7(e) of Executive Order 13526).

- The Mosaic theory is also available to withhold information under any other FOIA exemption.

#### Criteria:

- Mosaic theory applies to material which, when aggregated and discussed in the context of other responsive information, reveals other underlying facts, associations, or relationships that are protected
- Protected information need not be compiled in a single document
- Mosaic theory is not used to protect readily available information, such as information that is in widely available publications or on the Internet.
- Mosaic theory may be used for information considered “practically obscure”, such as information that was public in the past but is now relatively unavailable to the public.
- Applies to information that has been wrongfully leaked and is not confirmed by the agency; thus, it would not be considered publicly available.
- Conclusive proof of compromise or jeopardy of protected is required.

Waiver by Prior Disclosure: Mosaic theory is not used to limit the release of information already disclosed; however, material that is merely similar may be subject to protection.

## Exhibits

**Exhibit A:** [NRC FORM 510 "Personal Records Checklist"](#)

**Exhibit B:** Fee Categories

<b>Fee Categories</b>	<b>Search</b>	<b>Review</b>	<b>Duplication</b>
<b>Commercial Use</b>	Charge	Charge	Charge
<b>Educational Institution</b>	No charge (N/C)	N/C	N/C for first 100 pages
<b>General, Public and All Others</b>	NC for first 2 hours	N/C	N/C for first 100 pages
<b>News Media</b>	N/C	N/C	N/C for first 100 pages
<b>Noncommercial/ Scientific Organizations</b>	N/C	N/C	N/C

**Exhibit C:** Marking Redactions in Electronic Records (Adobe)



Adobe Cheat Sheet.docx

**Exhibit D:** [NRC FORM 511 "Program Office Response to a FOIA Request"](#)

**Exhibit E:** [FOIA Processing Guidance for Investigation and Allegation Related Material \(see page 328\)](#)

**Exhibit F:** Example of Out-of-Scope Markings



Out of Scope Example.pdf

**Exhibit G:** [NRC Form 496 "Report of Staff Resources for Processing FOIA Requests"](#)