



governmentattic.org

"Rummaging in the government's attic"

Description of document: Nuclear Regulatory Commission (NRC) Policy on Sensitive Internal Information, 2019

Requested date: 2019

Release date: 18-July-2019

Posted date: 21-October-2019

Source of document: FOIA Request
U.S. Nuclear Regulatory Commission
FOIA Officer
Mailstop: T-2 F43
Washington, DC 20555-0001
Fax: 301-415-5130
Email: FOIA.resource@nrc.gov

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: DoNotReply-NRCfoia <DoNotReply-NRCfoia@regulations.gov>
Sent: Thu, Jul 18, 2019 2:54 pm
Subject: Final Disposition, Request NRC-2019-000353

NRC-2019-000353 has been processed with the following final disposition: Full Grant.

Records were released to the public as a result of this request. You may retrieve these records immediately using the following link: [View Records Over the next 2 hours](#), these records are also being added to FOIAonline's search pages, further enabling you to retrieve these documents associated with your FOIA request at any time.

RESPONSE TO FREEDOM OF
INFORMATION ACT (FOIA) REQUEST

2019-000353

1

RESPONSE
TYPE☐

INTERIM

☒

FINAL

REQUESTER:

DATE:

07/18/2019

DESCRIPTION OF REQUESTED RECORDS:

A copy of the records marked "non-responsive" in the response to NRC-2019-000221

PART I. -- INFORMATION RELEASED

- ☐ The NRC has made some, or all, of the requested records publicly available through one or more of the following means: (1) <https://www.nrc.gov>; (2) public ADAMS, <https://www.nrc.gov/reading-rm/adams.html>; (3) microfiche available in the NRC Public Document Room; or FOIA Online, <https://foiaonline.gov/foiaonline/action/public/home>.
- ☒ Agency records subject to the request are enclosed.
- ☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (See Part I.D -- Comments) for a disclosure determination and direct response to you.
- ☐ We are continuing to process your request.
- ☐ See Part I.D -- Comments.

PART I.A -- FEES

AMOUNT

\$0.00

- ☐ You will be billed by NRC for the amount indicated.
- ☐ You will receive a refund for the amount indicated.
- ☐ Fees waived.
- ☒ Since the minimum fee threshold was not met, you will not be charged fees.
- ☐ Due to our delayed response, you will not be charged search and/or duplication fees that would otherwise be applicable to your request.

PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE

- ☐ We did not locate any agency records responsive to your request. *Note:* Agencies may treat three discrete categories of law enforcement and national security records as not subject to the FOIA ("exclusions"). See 5 U.S.C. 552(c). This is a standard notification given to all requesters; it should not be taken to mean that any excluded records do, or do not, exist.
- ☐ We have withheld certain information pursuant to the FOIA exemptions described, and for the reasons stated, in Part II.
- ☐ Because this is an interim response to your request, you may not appeal at this time. We will notify you of your right to appeal any of the responses we have issued in response to your request when we issue our final determination.
- ☐ You may appeal this final determination within 90 calendar days of the date of this response. If you submit an appeal by mail, address it to the FOIA Officer, at U.S. Nuclear Regulatory Commission, Mail Stop T-6 A60M, Washington, D.C. 20555-0001. You may submit an appeal by e-mail to FOIA.resource@nrc.gov. You may fax an appeal to (301) 415-5130. Please be sure to include on your submission that it is a "FOIA Appeal." Only a pre-registered user may file an appeal through FOIA Online, <https://foiaonline.gov/foiaonline/action/public/home>. A user who has not registered an account prior to filing the initial FOIA request may still submit their appeal by one of the above mentioned options.

PART I.C -- REFERENCES AND POINTS OF CONTACT

You have the right to seek assistance from the NRC's FOIA Public Liaison by submitting your inquiry at <https://www.nrc.gov/reading-rm/foia/contact-foia.html>, or by calling the FOIA Public Liaison at (301) 415-1276.

If we have denied your request, you have the right to seek dispute resolution services from the NRC's Public Liaison or the Office of Government Information Services (OGIS). To seek dispute resolution services from OGIS, you may e-mail OGIS at ogis@nara.gov, send a fax to (202) 741-5789, or send a letter to: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001. For additional information about OGIS, please visit the OGIS website at <https://www.archives.gov/ogis>.



**RESPONSE TO FREEDOM OF
INFORMATION ACT (FOIA) REQUEST**

2019-000353

1

RESPONSE
TYPE

☐

INTERIM

☒

FINAL

PART I.D -- COMMENTS

Signature - Freedom of Information Act Officer or Designee

Karen E. Danoff

Digitally signed by Karen E. Danoff
Date: 2019.07.18 13:08:02 -04'00'

You are here: [Home](#) » [Offices](#) » [SUNSI](#) » Sensitive Internal Information

[SUNSI Home](#) [Allegation](#) [CEII](#) [External Govt & Intl Agencies](#)
[Investigation](#) [Privacy Act/PII](#) [Proprietary](#) [Security Related](#) [Sensitive Internal](#)

Sensitive Internal Information

Table of Contents

- [Applicable Document Categories](#)
- [Authority to Designate](#)
- [Access](#)
- [Marking](#)
- [Cover Sheet](#)
- [Reproduction](#)
- [Processing on Electronic Systems](#)
- [Use at Home](#)
- [Use While Traveling or Commuting](#)
- [Physical Copy Transmission](#)
- [Electronic Copy Transmission](#)
- [Storage](#)
- [Destruction](#)
- [Decontrol Authority](#)

APPLICABLE DOCUMENT CATEGORIES

Attorney-Client Privilege

Attorney Work Product

Includes any predecisional information that rises to a level of sensitivity to justify it being protected as SUNSI. As such SII includes predecisional enforcement information but can also include other types of predecisional information. A subject matter expert should make a determination whether the specific predecisional information rises to a level that requires protecting it as SUNSI.

Sensitive - Not For Distribution (Except to Commission Adjudicatory Employees in Accordance with 10 CFR 2.348)

Information submitted to the Commission marked "Sensitive"

Source selection information other than proprietary information

AUTHORITY TO DESIGNATE

For NRC originated information, originator proposes – signer approves.

For NRC received information, office principally responsible for the information.

ACCESS

**Who may
have access?**

NRC employees or NRC contractor employees who have a need-to-know the information to perform their official duties.

MARKING

**What
documents
should be
marked?**

Mark all pages of all documents.

**Who may
authorize
document
marking?**

Originator, supervisor, or principal recipient.

**How should
a document
be marked?**

Mark at top and bottom of each page.

Mark as "**Official Use Only – Sensitive Internal Information**"

OR use more specific markings, as illustrated in the following examples:

For Attorney-Client Privilege: "**Official Use Only -- Attorney-Client Privilege**"

For Attorney Work Product: "**Official Use Only – Attorney Work Product**"

	<p>For Predecisional Enforcement Information: "Official Use Only – Predecisional Enforcement Information"</p> <p>For Adjudicatory Material: "Official Use Only – Adjudicatory Material"</p>
When is portion or page marking required?	<p>Not required.</p>

COVER SHEET

When should a cover sheet be used?	<p>Not required.</p> <p>Note: Use of the green "Official Use Only" cover sheet has been discontinued.</p>
What cover sheet is used?	<p>Not applicable.</p>

REPRODUCTION

How many copies may be made?	<p>Reproduction is limited to the number of copies needed for official use unless document contains restrictions.</p> <p>Copies must clearly show the original markings.</p> <p>Note: Where restrictions are imposed on reproduction, the employee must also ensure that there are no non-authorized copies residing in electronic systems, such as on the network drive, local hard drive, printers, copiers, or any other electronic medium.</p>
-------------------------------------	---

PROCESSING ON ELECTRONIC SYSTEMS

On what information	<p>NRC LAN and other systems authorized to operate by the NRC under MD 12.5, "NRC Cybersecurity Program."</p>
----------------------------	---

systems may the document be processed?

Is encryption required while data is at rest?

OMB has directed that all sensitive information be encrypted both at rest (electronically stored) and during transmission. NRC is working to implement the capability to automatically encrypt data at rest within NRC facilities. Any SUNSI that is outside of NRC facilities must be encrypted at rest.

May the information be processed in ADAMS?

Sensitive Internal Information may be entered into the ADAMS Main Library and must be profiled as Non-Publicly Available and Sensitive. Assign access rights to user groups with a need to access the information to perform their official duties. ADAMS Sensitivity Code: A.7 Note: Sensitive Internal Information has two (2) sub-categories within the A.7 sensitivity code. Therefore, you must select the proper A.7 based on the following criteria:

Sensitive Internal Information - No Periodic Review Required - contains attorney-client privilege, attorney work product, or predecisional enforcement information.

Sensitive Internal Information - Periodic Review Required - contains all other Sensitive Internal Information

.....

USE AT HOME

May I use the document at home?

Yes. Abide by the following requirements:

Employees are prohibited from using, handling, and storing the information at their residences and on personally owned devices or sending information to non-NRC email addresses (e.g., personal email accounts).

Occasional use at an employee's residence requires approval of the employee's immediate supervisor or above.

Electronic work from home must use an NRC computer or an NRC authorized capability, such as BYOD or CITRIX.

To ensure that the information is not viewed or accessed inadvertently or willfully by a person not authorized access, the

employee must ensure that the information cannot be seen by a family member, guest, or any other individual who is not authorized access.

Employees are prohibited from processing SUNSI on personally owned computers unless connected to and working within CITRIX, the NRC Broadband Remote Access System. Employees are prohibited from downloading or storing SUNSI to the hard drive of a personally owned computer when connected to and working within CITRIX. Employees are also prohibited expressly from processing SUNSI on personally owned computers even when an encrypted floppy disk, CD, DVD, or thumb drive is the storage media.

Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX, (2) an NRC-issued laptop with NRC-approved encryption software, or (3) using an NRC authorized solution such as BYOD.

It is discouraged to take hard-copy material to private residences. If hard copy material is taken home, it must be returned to an NRC facility and stored and/or destroyed according to the instructions provided in this guidance.

May I use the information at home under the NRC Flexible Workplace Program?

Yes. Abide by the following requirements.

If you are approved to work at home under the NRC Flexible Workplace Program, use in accordance with standards set forth in NRC Form 624, Flexible Workplace Program Participation Agreement.

To ensure that the information is not viewed or accessed inadvertently or willfully by a person not authorized access, the employee must ensure that the information cannot be seen by a family member, guest, or any other individual who is not authorized access.

Employees are prohibited from processing SUNSI on personally owned computers unless connected to and working within CITRIX, the NRC Broadband Remote Access System. Employees are prohibited from downloading or storing SUNSI to the hard drive of a personally owned computer when connected to and working within CITRIX. Employees are also expressly prohibited from processing SUNSI on personally owned computers even when an encrypted storage media is employed.

Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX or (2) an NRC-issued laptop with NRC-approved encryption software, or (3) using an NRC authorized solution such as BYOD.

USE WHILE TRAVELING OR COMMUTING

May I use the information while on official travel or commuting to or from work?

Yes. Abide by the following requirements:

Use of the information is discouraged while traveling on public transportation. To ensure that the information is not viewed or accessed inadvertently or willfully, the employee must ensure that it cannot be seen by persons not authorized access.

Particular care should be taken on a public conveyance or in waiting rooms where others may be sitting and standing in close proximity to where the information is being used.


Individuals should hand carry protected information during travel only if other means for transmitting the information, e.g., mailing ahead, secure information sharing, are not readily available or are operationally unacceptable. If hand carrying is determined to be the best transport method, care must be exercised to ensure that the information is not compromised through loss or inadvertent access.

Information must be kept in the traveler's personal possession to extent possible, and stored, appropriately wrapped, in hotel security facilities if possible.

Information must not be saved/stored on a personally owned computer. Work must be performed on an encrypted laptop computer or other encrypted mobile IT device to preclude unauthorized access if the laptop or device is lost or stolen..

The information should be returned to an NRC authorized storage location at the earliest possible opportunity.

PHYSICAL COPY TRANSMISSION

<p>May I transmit paper or electronic media including CD-ROM, disk or tape?</p>	<p>Yes. Abide by the following requirements:</p> <p>Inside the NRC:</p> <p>Electronic submissions, including CD-ROMs, submitted to the NRC should follow the E-Rule "Guidance for Electronic Submission to the Agency," available on NRC's external Web site at: (http://www.nrc.gov/site-help/electronic-sub-ref-mat.html).</p> <p>Outside the NRC: Information may be transmitted by –</p> <p>NRC Messenger/NRC contractor messenger.</p> <p>U.S. Postal Service: First Class Mail, Registered Mail, Express Mail, Certified Mail.</p> <p>Hand-carried by any individual authorized access to the information. That individual shall retain the information in his or her possession to the maximum extent possible unless they place the document in the custody of another person authorized access.</p> <p>Approved commercial express carriers (time-sensitive material only; use NRC Form 420); Transmit in single opaque envelope.</p> <p>Other means approved by OIS and the Director, Division of Facilities and Security, ADM.</p> <p>Incoming to the NRC: Electronic submissions, including CD-ROMs, submitted to the NRC should follow the E-Rule "Guidance for Electronic Submission to the Agency," available on NRC's external Web site at: (http://www.nrc.gov/site-help/electronic-sub-ref-mat.html)</p> <p>Encryption:</p> <p>All electronic media (CD-ROM, disk, tape, hard drives, thumb drives, etc.) must be encrypted in accordance with MD 12.5.</p> <p style="text-align: center;"></p>
<p>ELECTRONIC COPY TRANSMISSION</p>	
<p>May I transmit the document electronically by e-mail or fax?</p>	<p>Yes. Abide by the following requirements:</p> <p>Inside the NRC (including Regions): Information may be emailed or faxed.</p> <p>Electronic transmissions (e.g., e-mail, fax) outside the NRC must be encrypted in accordance with MD 12.5</p>

Outside the NRC: Information may be transmitted by –

Fax: May use non-secure facilities where it is confirmed that a recipient who is authorized to access the information will be present to receive the information.

E-Mail: All SUNSI information must be encrypted during transmission outside of the internal network as stated in [MD 12.5](#). Please follow the guidance outlined in the Office of the Chief Information Officer issued [announcement dated February 9, 2017](#).

Use of portals that encrypt the information during transmission, such as "BOX" are highly encouraged.

Otherwise, transmit a physical copy in the manner set forth above.

Electronic files must contain appropriate markings.



STORAGE

Inside the NRC (Headquarters and Regional Offices): Store in non-locking or locking container at the end of each business day or when not in use.

Outside the NRC (Resident Inspector Sites): Store in key locked desks or other key locked containers.

On NRC Electronic Systems: May be stored on NRC encrypted computer systems authorized to operate under [MD 12.5](#).



DESTRUCTION

Official Record Version: Destroy in accordance with NRC Comprehensive Records Disposition Schedule (NUREG-0910).

Non-Official Record Copies: Destroy copies other than the official record version by any means that prevents reconstruction in whole or part, including the following methods:

Using an ADM/DFS approved shredder that has been approved to destroy classified information, Safeguards Information, SUNSI, and Controlled Unclassified Information (CUI).

Placing in a Sensitive Unclassified Waste Disposal Container.

Tearing into one-half inch pieces or smaller (in all dimensions) and dispose of in a waste receptacle.

Burning, pulping, pulverizing, or chemical decomposition.

Electronic Data: Use NRC authorized destruction methods in accordance with [MD 12.5](#).



DECONTROL AUTHORITY

Originating office or office primarily responsible for the information.



CONTENT OWNER

Page content maintained by: SUNSI.Resource@nrc.gov