UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

FEB 13 2018

IN RESPONSE REFER TO:
NRC-2018-000275/NRC-2018-000062
NRC-2018-000302/NRC-2018-000048

Mr. Julian Tarver
Washington State Penitentiary IMU South H-2
1313 N 13th Avenue
Walla Walla, WA 99362

Dear Mr. Tarver:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your letters dated December 15 and 28, 2017, in which you appealed the agency's December 7 and 19, 2017, responses related to your November 9 and 10, 2017, Freedom of Information Act (FOIA) requests, NRC-2018-000048 and NRC-2018-000062. Your requests sought records reflecting the history, overview or description, of the former Foreign Intelligence Information [FII] program and records reflecting the disposition of the FII program's records. You appealed the adequacy of the searches in both requests.

Acting on your appeal, I have considered the matter and have determined that your appeals are granted.

At the time of the FOIA Office's receipt of both requests, the Offices of International Programs [OIP] and Nuclear Security & Incident Response [NSIR] were tasked to search for records. The only record that was located, Yellow Announcement No. 040, dated May 28, 2003, which reflected the NRC's decision to discontinue the FII program, was provided to you. After receiving your appeals, we tasked OIP and NSIR to conduct new searches. These offices again reported finding no additional records; however, we learned that, prior the establishment of NSIR in April 2002, the FII program fell under the jurisdiction of the Office of Administration [ADM]. As such, ADM was tasked to search. It identified two records maintained in ADAMS that appear to be responsive to your requests. Although both records constitute internal deliberations and recommendations of NRC staff that preceded the agency's decision to discontinue the FII program, as a matter of discretion, we are releasing the records in their entirety. They are enclosed. Finally, given the age of the FII program, we reached out to our Records Office to ascertain whether FII program-related records were transferred to the National Archives & Records Administration [NARA] for permanent retention; the Records Office did not find any documentation that any FII program records were transferred to NARA. Accordingly, I am satisfied that the NRC has no other records responsive to your requests.

This is the final agency decision. As set forth in the FOIA (5 U.S.C. 552(a)(4)(B)), you may seek judicial review of this decision in the district court of the United States in the district in which you reside or have your principal place of business. You may also seek judicial review in the district in which the agency's records are situated or in the District of Columbia.

The 2007 FOIA amendments created the Office of Government Information Services (OGIS) to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a nonexclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. You may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
732 North Capitol Street, NW
Washington, D.C. 20401
Email: ogis@nara.gov
Telephone: 202-741-5770
Toll-free: 1-877-684-6448
Fax: 202-741-5769

Sincerely,

David J. Nelson
Chief Information Officer
Office of the Chief Information Officer

February 11, 2003

MEMORANDUM TO: Michael L. Springer, Director
Office of Administration

FROM: Roy P. Zimmerman, Director **/RA/**
Office of Nuclear Security and Incident Response

SUBJECT: INTENT TO ELIMINATE THE NRC FOREIGN INTELLIGENCE INFORMATION (FII) PROGRAM

As part of an ongoing comprehensive review of security and safeguards, the Office of Nuclear Security and Incident Response (NSIR) is reviewing whether the NRC Foreign Intelligence Information (FII) program provides significant security value commensurate with measures necessary to maintain the program. Our preliminary analysis (attached) suggests it does not. Therefore, I am considering eliminating the FII program as an NRC requirement.

The NRC FII program was originally established in the 1970s to assure the Intelligence Community that the NRC, as a new recipient of intelligence information, would strictly control access and handling of the information in order to receive it. Much has changed in the years since the FII program began. Executive orders and federal regulations specifically address security requirements for the handling of classified information, to which the NRC must adhere. As an NRC creation, the FII program goes beyond the designations of the Executive Order on classified information in this regard. Terrorist activities and the potential dangers radiological materials pose have led to a greater need for intelligence information by many agencies. The NRC is one of these agencies and it currently receives classified information, including intelligence information, on a routine basis. The NRC is no longer a new recipient of classified information needing to implement special measures in order to ensure proper information security. In addition, the FII program requires special access lists, extra controls, extra markings/cover sheets, extra training, and special handling and destruction which have led to additional work and unnecessary costs. Based on the aforementioned reasons, it appears that the NRC can effectively maintain information security and properly adhere to Federal requirements without an FII program.

I am informing you of my intention because the elimination of the FII program would impact one method your office uses to identify some employees for drug testing. The elimination of the FII program would lead to the elimination of the FII list, a list of all NRC personnel approved for FII access. The FII list is currently maintained by INFOSEC and provided to the Drug Testing Coordinator and HR on a monthly basis to identify some, but not all, of the employees that make up drug testing Category 3, as described in NUREG/BR-0134, Rev. 1. In lieu of the FII list, the NRC might be able to use the list of NRC employees with Q clearance (access to Top Secret National Security Information and Secret Restricted Data) or just employees with access to sensitive compartmented information. The INFOSEC staff has discussed this issue with members of your Security Branch.

M. Springer

I ask that you inform me of any objection to the elimination of the FII program by February 26, 2003, to support a final decision on the program.

You may contact Lynn Silvious, 415-2214, if you have questions.

Attachment: FII Analysis

cc: WKane
PNorry
CPaperiello
SCollins
MVirgilio
AThadani
PBird
KCyr
Avietti-Cook
TMartin
CStone

M. Springer

I ask that you inform me of any objection to the elimination of the FII program by February 26, 2003, to support a final decision on the program.

You may contact Lynn Silvious, 415-2214, if you have questions.

Attachment: FII Analysis

cc: WKane
PNorry
CPaperiello
SCollins
MVirgilio
AThadani
PBird
KCyr
Avietti-Cook
TMartin
CStone

Distribution
NSIR/DNS/ISS RF
NSIR RF

ADAMS: Yes **Non-Publically Available** **Non-Sensitive** Initials MVW
DOCUMENT NAME: C:\ORPCheckout\FileNET\ML030290007.wpd ML: 030290007
* See previous concurrence
C = Copy without attachment/enclosure E = Copy with attachment/enclosure N = No copy.

OFFICE	NSIR/DNS/ISS	E	NSIR/DNS/ISS:C	N	NSIR/DIRO		NSIR/DNS:DD	
NAME	MVan Winkle*		ALSilvious*		RWessman*		CHaney	
DATE	01/ 29 /03		01/ 29 /03		01 / 29 /03		02 / 06 /03	
OFFICE	NSIR/DNS:D		NSIR		NSIR			
NAME	GTracy		MWeber		RZimmerman			
DATE	02/ 06 /03		/ /		02 / 11 /03			

OFFICIAL RECORD COPY

January 27, 2003

MEMORANDUM TO: Michael F. Weber, Deputy Director
Office of Nuclear Security and Incident Response

FROM: A. Lynn Silvious, Chief /RA/
Information Security Section
Division of Nuclear Security
Office of Nuclear Security and Incident Response

SUBJECT: FUTURE USE OF FOREIGN INTELLIGENCE INFORMATION (FII), ACTION ITEM NSIR-03-0071

Attached is my recommendation in response to action item NSIR-03-0071 (formerly NSIR 02-0037), Future Use of Foreign Intelligence Information.

Attachment: FII Recommendation

cc: GTracy
CHaney
CStone

Contact: Mark Van Winkle
415-2212

January 27, 2003

MEMORANDUM TO: Michael F. Weber, Deputy Director
Office of Nuclear Security and Incident Response

FROM: A. Lynn Silvious, Chief /RA/
Information Security Section
Division of Nuclear Security
Office of Nuclear Security and Incident Response

SUBJECT: FUTURE USE OF FOREIGN INTELLIGENCE INFORMATION (FII), ACTION ITEM NSIR-03-0071

Attached is my recommendation in response to action item NSIR-03-0071 (formerly NSIR 02-0037), Future Use of Foreign Intelligence Information.

Attachment: FII Recommendation

cc: GTracy
CHaney
CStone

Contact: Mark Van Winkle
415-2212

Distribution:

NSIR/DNS/ISS RF
NSIR-03-0071

ADAMS Yes No Initials mvw ML: 030270310
Publicly Available Non-Publicly Available Sensitive Non-Sensitive
DOCUMENT NAME: C:\ORPCheckout\FileNET\ML030270310.wpd
C = Copy without attachment/enclosure E = Copy with attachment/enclosure N = No copy

OFFICE	NSIR/DNS/ISS	E	NSIR/DNS/ISS:C	
NAME	MVan Winkle		ALSilvious	
DATE	01/ 27 /03		01/ 27 /03	

OFFICIAL RECORD COPY

ATTACHMENT 1

PURPOSE:

To discuss the merits of the NRC Foreign Intelligence Information (FII) program.

ISSUE:

Determine if the NRC FII program provides information security value commensurate to required control measures.

ALTERNATIVES:

Alternative 1:	Continue with the current NRC FII program.
Alternative 2:	Maintain current NRC FII employee identification, training, and access control requirements, but eliminate FII as a criterion for drug testing.
Alternative 3:	Replace the current NRC FII program with an information security requirements and awareness education program. Maintain the requirement to identify FII with an internal-NRC marking/cover sheet to alert personnel who have access to FII.
Alternative 4:	Totally eliminate the NRC FII program and amend criteria for drug testing.

BACKGROUND:

In December 2002, the Deputy Director of NSIR asked INFOSEC to consider whether the NRC FII program provided security value commensurate with the required control measures of the program as part of an ongoing comprehensive security and safeguards review.

The NRC FII program is an NRC creation that goes beyond the official designations in the Executive Order on classified information. The NRC uses FII as the term to designate classified information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, except for counterintelligence information as it relates to terrorist activities. FII markings and cover sheets are used to separately identify it from other classified information (enrichment technologies, security at Category I facilities, and etc.) in order to help ensure it will not be released to any agency outside the NRC regardless of access authorization.

In order to acquire intelligence information in the mid-1970s, the NRC assured the Intelligence Community (IC) that limitations would be placed on the distribution of information since the NRC was not, and is not now, a member of the IC. Non-IC agencies are not permitted to share classified information with any organization without the approval of the originating agency. MOUs with the IC specifically limited access to designated NRC officials (by name and position). The usefulness of these MOUs has long since past. The NRC began to receive intelligence information from the IC as early as 1975.

Initial NRC program requirements to guard against the release of intelligence information (as called FII) outside the NRC were set forth in a bulletin. In 1979, FII requirements were formalized into NRC security directives.

In 1985, INFOSEC conducted a study of the NRC FII program, including how other non-IC agencies handled intelligence information. This study led to the merging of NRC FII requirements into the management directive on classified information, currently MD 12.2 (Attachment 1a).

In May 1995, while preparing a list of items required to be accomplished in conjunction with the implementation of Executive Order 12958, INFOSEC noted that the NRC needed to "Determine if FII should remain in effect, or whether it really constituted an unauthorized special access program (SAP)." In accordance with Section 4.4 of Executive Order 12958, the NRC does not have the authority to establish a SAP. Section 5.7 of the Order authorizes the Director of the Information Security Oversight Office (ISOO) to sanction agencies for violations of the Order.

In June 1995, INFOSEC delineated to the Director of Security why the handling of FII in a manner befitting a SAP was not cost effective, did not significantly enhance the security of the information, and was possibly in contravention to the Order.

The Director of Security requested INFOSEC to discuss the issue with the DoD SAP policy and program manager. The DoD manager stated that the most compelling reason to see the NRC FII program as a SAP was the requirement for "Q" access authorization to access FII of any classification level (confidential - top secret). Based on that information and the NRC environment at the time, a subsequent revision of MD 12.2 changed access authorization requirements to be commensurate with the level of classification indicated on the intelligence information.

The ISOO, which has responsibility for enforcement of SAP prohibition provisions of the Executive Order, was provided a copy of the revised MD 12.2 for its review. No adverse comment was received to indicate an unauthorized SAP program existed at the NRC.

NRC personnel may have access to FII if they meet the following conditions as found in MD 12.2:

- A requirement for FII in the performance of their official duties (need to know)
- Proper access authorization
- Identified by a Commissioner, an office director, regional administrator, or DFS as having a need-to-know in the performance of his/her duties (INFOSEC annually requests a need-to-know FII listing from NRC organizations and maintains a complete listing for the NRC)
- Attendance at, or reading of, the FII Security Education and Awareness Briefing produced and presented by INFOSEC to specifically address the controls and handling required for FII

Individuals must sign a locally-produced access record each time they access FII, creating a list of personnel who have had access to information. Each record must be kept for 2 years, even if the document has been destroyed.

Office directors and regional administrators must inform INFOSEC when an employee–

- No longer requires FII in the performance of his/her official responsibilities
- Announces his/her intention to leave the NRC or his/her employment is terminated
- Security considerations dictate the termination of need-to-know access by the Director, DFS

Contractors, consultants, and other persons not employed by the NRC are not authorized access to FII in the NRC. Therefore, disposal of FII in the common containers used for the collection of sensitive and classified materials is prohibited due to access by contractor security guards.

The NRC FII program became tied to the NRC drug testing program when access to FII was identified as a criterion in the NRC Drug-Free Workplace Plan, NUREG/BR-0134, Rev 1, for establishing "pools" of employees for drug testing. The Office of National Drug Control Policy issued guidance on Executive Order 12564 (drug testing) requiring federal agencies to establish employee pools when implementing drug testing. This led to INFOSEC continually updating the FII list and providing it to the Drug Testing Coordinator and HR on a monthly basis.

In 1982, Executive Order 12356 established the "Third Agency Rule". Executive Order 12958 (1995) retained the provision and provides that "classified information originating in one U.S. department or agency shall not be disseminated beyond any recipient agency without the consent of the originating agency." Typically, the NRC will not disseminate classified information to any department or agency outside the NRC without the consent of the originating agency.

DISCUSSION:

As previously stated, the purpose of this paper is to discuss the merits of the NRC FII program and the issue is to determine if the program provides information security value commensurate to required control measures. Can alternative procedures provide adequate security and reduce workloads and/or eliminate unnecessary work constraints? Facts with positive and negative aspects of each alternative follow to assist in making that determination.

Approximately 500 NRC employees are pooled in the drug testing category that is comprised, in part, by the FII criterion. Of these 500 NRC employees, 350 are specifically, but not exclusively, pooled due to the FII program. Employees with access to Sensitive Compartmented Information (SCI) or who require access more than once a year to classified information also are required to be pooled in the same category as employees who have access to FII. This pool is termed Category 3 in NUREG/BR-0134, Rev. 1 (Attachment 1b). The continuation, modification, or elimination of the NRC FII program would not eliminate

specific individuals or reduce the number of NRC employees currently in Category 3. The information the NRC terms FII is always classified and would still be disseminated in some fashion to NRC employees that have access authorization and a need-to-know, thereby keeping these employees in drug testing pool Category 3. However, eliminating the NRC requirement to identify and list individuals that have access to "FII" would make it difficult for the NRC to accurately identify all individuals in Category 3. The FII list, along with the list of 122 individuals that have access to SCI (maintained by INFOSEC), are the only tangible methods of identifying employees in Category 3. The INFOSEC staff is unaware of any current method to identify employees that may have access to classified information that is not SCI or for what the NRC terms FII. These types of classified information would include enrichment technologies, security at Category I facilities, and etc.

Alternative 1, Continue with the current NRC FII program:

- Established to assure the IC that the NRC would securely handle intelligence information
- As currently established, no major change needed to directives or training
- Proven to be an effective program maintaining information security
- The FII list tangibly identifies NRC employees who may have a need-to-know
- The NRC FII program requires employees to distinctively mark FII, clearly identifying it as information that must be separately handled and destroyed
- Locally-produced access records list who has had access to FII
- Helps to reinforce the "Third Agency Rule" as it pertains to releasing classified information outside the NRC.
- Workload intensive
    - Commissioners, office directors, regional administrators, or DFS must initially identify individuals needing access to FII and continually update that information when an employee's need to know no longer exists, announces his/her intention to resign or his/her employment is terminated, or security considerations dictate termination of need-to-know access by DFS.
    - Special training required by INFOSEC
    - FII list must be updated by INFOSEC and provided to the Drug Testing Coordinator and HR on a monthly basis.
    - Establishes a criterion for drug testing requiring tracking by the Drug Testing Coordinator and HR
- Defacto SAP

Alternative 2, Maintain current NRC FII program, but eliminate FII as a criterion for drug testing:

- Would likely be an effective program maintaining information security
- Would provide a tangible list of employees who may have a need-to-know FII
- Would require NRC employees to distinctively mark FII, thereby clearly identifying it as information that must be separately handled and destroyed
- Locally-produced access records would provide a method to list who has had access to FII
- Would help to reinforce the "Third Agency Rule" as it pertains to releasing classified information outside the NRC.
- Some residual workload would remain
  - Commissioners, office directors, regional administrators, or DFS would initially identify individuals needing access to FII and continually update that information when an employee's need to know no longer exists, announces his/her intention to resign or his/her employment is terminated, or when security considerations dictate termination of need-to-know access by DFS.
  - Special training would be required by INFOSEC
  - FII list maintenance by INFOSEC
- Would be a defacto SAP
- Would require a rewrite or change supplement to NUREG/BR-0134 to eliminate FII as a drug testing criterion. Changes to federal agency drug plans must be approved by the Department of Health and Human Services

Alternative 3, Replace the current NRC FII program with an information security requirements and awareness education program. Maintain the requirement to identify FII with a distinctive marking/cover sheet to alert employees that have access to FII

- Would require NRC employees to distinctively mark FII, thereby clearly identifying it as information that must be separately handled and destroyed
- "Third Agency Rule" would apply to the release of classified information outside the NRC
- Would eliminate the need for INFOSEC to maintain and update an FII list
- Would eliminate the need for Commissioners, office directors, regional administrators, or DFS to initially identify individuals needing access to FII and to

continually update that information when an employee's need to know no longer exists, announces his/her intention to resign or his/her employment is terminated, or when security considerations dictate termination of need-to-know access by DFS

- Would eliminate all drug testing program requirements related to FII (list updates, tracking, and etc) without eliminating specific individuals or reducing the number of NRC employees currently in the Category 3 drug testing pool

- Would eliminate need to maintain access records and, subsequently, would not allow for verification of who has had access to information

- Would eliminate SAP concerns

- Would not provide a tangible list of employees who may have a need-to-know

- New training requirements would need to be developed and implemented

- Would require a revision of MD 12.2

Alternative 4, Totally eliminate the NRC FII program and amend drug testing criteria.

- "Third Agency Rule" would apply to the release of classified information outside the NRC

- Would eliminate the need for INFOSEC to maintain and update an FII list

- Would eliminate the need for Commissioners, office directors, regional administrators, or DFS to initially identify individuals needing access to FII and to continually update that information when an employee's need to know no longer exists, announces his/her intention to resign or his/her employment is terminated, or when security considerations dictate termination of need-to-know access by DFS

- Would eliminate all drug testing program requirements related to FII (list updates, tracking, and etc) without eliminating specific individuals or reducing the number of NRC employees currently in the Category 3 drug testing pool.

- Would require a rewrite or change supplement to NUREG/BR-0134 to eliminate FII references to drug testing. Changes to federal agency drug plans must be approved by the Department of Health and Human Services

- Would eliminate need to maintain access records and, subsequently, would not allow for verification of who has had access to information

- Would eliminate SAP concerns
- Would eliminate FII-specific training

- Collateral intelligence information would not be identified with a distinctive FII marking/cover sheet identifying it as information that must be separately handled and destroyed

- Would not provide a tangible list of employees who may have a need-to-know

- Would require a revision to MD 12.2

No resource adjustment to the NRC Five-Year Plan is anticipated with any alternative.

RECOMMENDATION:

The staff recommends Alternative 4. Rationale for its adoption follows.

The staff views the current FII program as a work intensive program, requiring extra markings/cover sheets, extra controls, extra training, and special handling and destruction beyond the requirements found in executive orders and federal directives. It does not provide significant security enhancements, commensurate with these measures, that could not be adequately achieved through the proper application of the existing executive orders and federal directives relating to the marking, handling, and destruction of classified information.

The NRC FII program was established to help ensure the NRC would not improperly release classified information outside the NRC. Proper adherence by NRC employees to the "Third Agency Rule" and federal directives would prevent improper releases in that regard.

Adoption of Alternative 4 would eliminate the need for Commissioners, office directors, regional administrators, or DFS to identify and delete individuals needing access to FII, and subsequently, the need for INFOSEC to maintain and update a list of those personnel. In addition, the NRC would no longer establish and file access records to identify personnel that had access to specific confidential and secret information. Again, the NRC access record requirement for confidential and secret information goes beyond federal requirements. The access requirements for SCI and top secret information would remain and are not addressed in, or impacted by, this paper. The need for INFOSEC to train NRC employees on specifics of the FII program would also cease.

The FII list currently maintained by INFOSEC provides an easy method of identifying many, but not all, personnel that are pooled in drug testing Category 3. As previously stated, eliminating the FII list would not eliminate specific individuals or reduce the total number of employees in Category 3. However, eliminating the list would make it difficult to identify existing personnel or new employees requiring drug testing, which still would be required, since they would likely access classified information more than once a year, a Category 3 criterion. Methods may need to be developed to identify all Category 3 members, or a re-categorization of drug testing pools may need to be considered. This issue was discussed with the Chief, Security Branch, DFS. She did not object to the elimination of the FII program, but she questioned how the NRC would identify applicable employees in Category 3 after the elimination of the FII program. Possibilities were discussed and the INFOSEC staff pledged to assist in developing a possible method if needed. In any event, a revision to NUREG/BR-0134 would eventually be required

after the elimination of the FII program. Current references to the FII program in NUREG/BR-0134 would become moot in the interim.

Eliminating the FII list would also result in the loss of a tangible method of identifying employees that may have a need-to-know. However, access to classified information should not be permitted carte blanche based on a list of names, but only should be permitted case by case based on an employee's duties relative to the content of the classified information (need-to-know) along with proper access authorization. Authorized individuals in possession of classified information make these determinations. SCI and SAPs are exceptions requiring lists of personnel that have been properly cleared into programs.

Adoption of Alternative 4 would eliminate concerns that the NRC FII program constitutes an unofficial SAP. In addition, the special requirements now in effect prohibiting cleared contract guards from destroying what the NRC calls FII would cease. All classified information would be handled and destroyed in accordance with current federal directives.

Part II and all other references to FII would be eliminated from MD 12.2 during its revision which is currently underway.

Educating applicable NRC employees will be necessary if any change occurs to existing information security programs. The staff views potential new training challenges as minor since the result will be the elimination of some current requirements without the addition of any new requirement.

In conclusion, it is the staff's view that the advantages that would be gained by the adoption of Alternative 4 would clearly out weigh disadvantages, without an inherent potential for security compromise.

ATTACHMENT 1