OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of NRC's Foreign Assignee Program

OIG-17-A-07
December 19, 2016

All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

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

OFFICE OF THE
INSPECTOR GENERAL

December 19, 2016

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

Nader Mamish
Director, Office of International Programs

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S FOREIGN ASSIGNEE PROGRAM
(OIG-17-A-07)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Foreign Assignee Program*.

The report presents the results of the subject audit. Following the December 14, 2016, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-17-A-07

December 19, 2016

Results in Brief

Why We Did This Review

Under the foreign assignee program, the Nuclear Regulatory Commission (NRC) invites peers from other nuclear safety regulators to obtain experience that would enhance safety programs and research programs worldwide, as well as promote exchange of technical information and expertise.

Foreign assignees remain employees of the sponsoring regulatory or research organization in their home country. Approximately 80 foreign nationals have worked as assignees at NRC since 2005, representing 21 countries.

The Office of International Programs (OIP) has primary responsibility for the foreign assignee program and coordinates with other offices through the process of onboarding a foreign assignee and during the assignment. In recent years, assignees have worked in various offices at NRC headquarters and in NRC regional offices.

The Office of the Inspector General (OIG) conducted this audit to assess whether the NRC foreign assignee program provides adequate information security.

Audit of NRC's Foreign Assignee Program

What We Found

Existing foreign assignee program policies establish controls for protection of and access to information within the foreign assignee program. However, improvements are needed to better implement policies and strengthen information security.

For example, information security requirements for the foreign assignee program are not implemented consistently, because there is no specific procedure to guide implementation of those requirements. As a result, program offices may not be able to maintain adequate information protection.

In addition, foreign assignees use a non-NRC, external email address while working at NRC. Foreign assignees do not have an NRC email address because that would require access to the internal local-area network and foreign assignees do not meet the access standard to use NRC's network. The use of external email presents a potential risk of an unintentional spillage of information that should be protected.

What We Recommend

The report makes recommendations to develop a procedure for security planning during the process of onboarding and hosting a foreign assignee and to provide a secure, cost-effective email for the use of foreign assignees at NRC. Management stated their agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ADM	Office of Administration
DFS	Division of Facilities and Security
EDO	Executive Director for Operations
IAEA	International Atomic Energy Agency
MD	Management Directive
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	Nuclear Regulatory Commission
NRO	Office of New Reactors
NRR	Office of Nuclear Reactor Regulation
NSIR	Office of Nuclear Security and Incident Response
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIP	Office of International Programs
RES	Office of Nuclear Regulatory Research
SUNSI	Sensitive Unclassified Non-Safeguards Information

I. BACKGROUND

The foreign assignee program has become a significant component in Nuclear Regulatory Commission (NRC) international activities, which entail participation in international research and safety and security programs. Established by the Atomic Energy Commission in 1974, the foreign assignee program has evolved based on global nuclear safety and regulatory developments and NRC priorities. Under the program, NRC invites peers from other nuclear safety regulators to obtain experience that would enhance safety programs and research programs worldwide, as well as promote exchange of technical information and expertise.

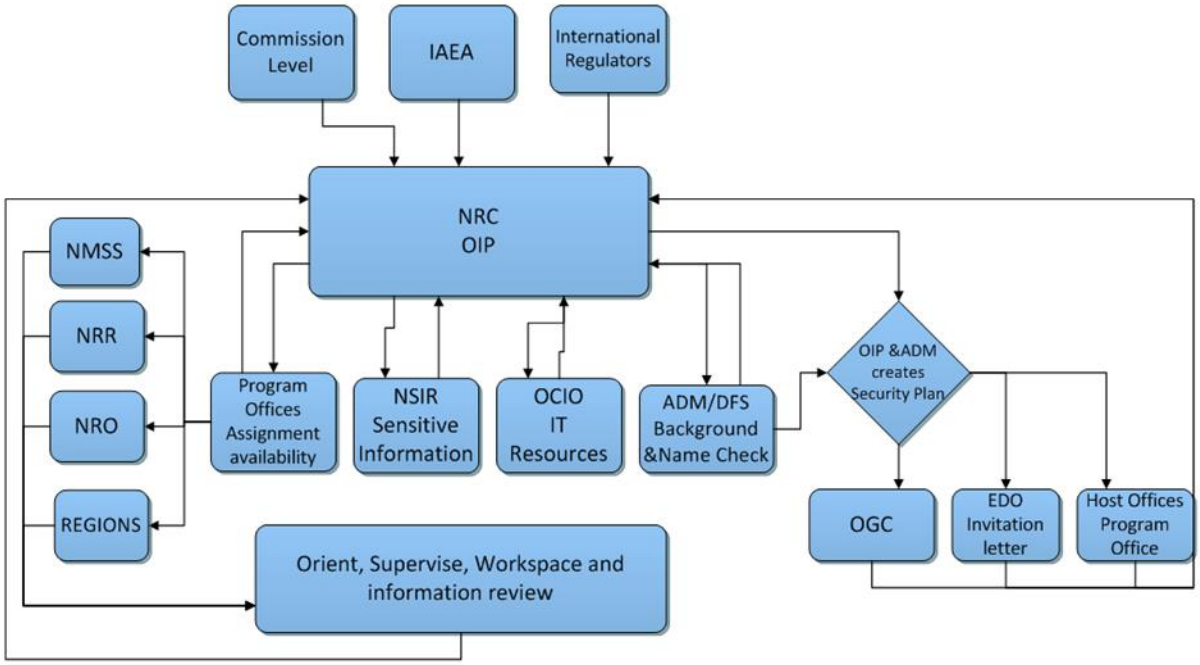
Foreign assignees, their interests, and the concerns of the foreign regulatory or research organizations that employ them vary considerably, reflecting a dynamic international environment. Foreign assignees remain employees of the sponsoring regulatory or research organization in their home country, and NRC resources for the foreign assignee program are largely limited to staff time to arrange, support, and supervise assignee projects. Approximately 80 foreign nationals have worked as assignees at NRC since 2005, representing 21 countries. NRC hosts eight to 12 assignees per year for assignments of up to 3 years. In recent years, assignees have worked in the Office of Nuclear Regulatory Research (RES), the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), the Office of Nuclear Material Safety and Safeguards (NMSS), and in NRC regional offices.

Responsible Offices and Coordination Process

The foreign assignee program involves many NRC offices. Figure 1 represents the coordination among responsible offices in the program.

The Office of International Programs (OIP) has primary responsibility for the foreign assignee program and coordinates with other offices through the process of onboarding a foreign assignee and for the duration of the assignment.

Figure 1: Foreign Assignee Coordination Process



Source: Office of the Inspector General (OIG).

OIP receives proposals for assignments from foreign regulatory counterparts, from the International Atomic Energy Agency (IAEA), or from NRC Commissioners. If an NRC program office identifies a suitable project based on a proposal, the Office of Administration (ADM), Division of Facilities and Security (DFS), requests a security check of Federal databases for information available about the potential assignee.

Once the security check returns no negative information, OIP, DFS, and the hosting program office develop a security plan for the foreign assignee. The Office of Nuclear Security and Incident Response (NSIR) approves any foreign assignee access to special classes of safeguards information. After review and concurrence by OIP, DFS, the host office, and the Office of the General Counsel (OGC), an invitation from the Executive Director for Operations (EDO) is issued to the foreign assignee's employer.

To prepare for an assignee's arrival, the host office selects and DFS approves a work space. The Office of the Chief Information Officer (OCIO) provides work technology, consisting of a desktop computer not connected to NRC's local-area network and limited connection to the

Internet through a guest network separated from NRC's local-area network. Upon arrival, the foreign assignee receives a distinctive access badge from DFS and is oriented to the security plan by OIP and the host office. The hosting program office supervises the assignee's work and information used during the assignment. At the conclusion of the assignment, DFS and the host office review and approve NRC information that the assignee used and wishes to remove from NRC.

II. OBJECTIVE

The audit objective was to assess whether NRC's foreign assignee program provides adequate information security.

III. FINDINGS

Existing program policies establish controls for protection of and access to information within the foreign assignee program. However, improvements are needed to better implement policies and strengthen information security by

A. Providing clear procedures to plan for and host foreign assignees.
B. Eliminating assignees' use of external email to perform NRC work.

A. Lack of Clear Procedures

NRC management is responsible for providing effective procedures to ensure consistent implementation of agency policies. However, information security requirements for the foreign assignee program are not implemented consistently, because there is no specific procedure to guide implementation of those requirements. As a result, program offices may not be able to maintain adequate information protection.

What Is Required

Management Responsible for Providing Procedures

NRC management is responsible for providing procedures to ensure consistent implementation of agency policies regarding security.

Management Responsibility

Federal standards designate management as responsible for providing procedures that serve as a mechanism to support efficient operations, reliable reporting and communication, and reasonable assurance that requirements are met. The U.S. Government Accountability Office *Standards for Internal Control in the Federal Government* (2014) states that effective procedures document control activities designed to achieve objectives and respond to risk, especially for complex processes. Management must communicate internally the information needed to achieve objectives. Guidance documents, used properly, can channel the discretion of agency employees and increase efficiency.

NRC Security Requirements

NRC policies for the foreign assignee program appear in Management Directives (MDs). MD 5.13, *NRC International Activities Practices and Procedures*, has a brief synopsis of the purpose of the program, processing of assignees, onboarding assignees, and supervision. The requirements for information security are published in the security MDs 12.1, *NRC Facility Security Program*; 12.3, *NRC Personnel Security Program*; and 12.5, *NRC Cybersecurity Program*. The directives assign responsibilities and establish requirements for the contents of security plans, supervision and monitoring of assignees, and access restriction to prevent unauthorized access to sensitive information.

Further, MD 12.3 has brief guidelines for the prevention of unauthorized access to classified or sensitive unclassified information by foreign assignees. According to MD 12.3, foreign assignee security plans must include the following elements:

- A description of the physical location of the assignment.
- Identification of specific areas to which the assignee is to be given unescorted access.
- An explanation of special badging.
- An explanation of restrictions on the use of NRC computing resources such as the local-area network.
- A discussion of the ways in which commercial or foreign proprietary information must be protected.
- Instructions on alerting co-workers about an assignee's presence and the assignee's restricted access, both physical and informational, including a Division of Facilities and Security (DFS) briefing.
- Assignment of a supervisor and an alternate.
- Requirement for monthly or quarterly progress reports from the assignee.
- Requirement for a mid-point interview by DFS of the assignee, the assignee's supervisors, and, as appropriate, the assignee's co-workers.

What We Found

Security Requirements Not Implemented Consistently

The information security requirements for the foreign assignee program are not implemented consistently.

Security Plan Inconsistencies

A review of 17 security plans from the last 3 years showed omissions of required elements in some plans and inconsistency in others. One of the plans OIG reviewed did not specifically name the branch chief as supervisor, as required by MD 12.3. Ten of the plans did not designate an alternate supervisor. Eight plans omitted the requirement that the branch chief must instruct staff on the contents of the assignee's security plan. None of the reviewed plans included instructions for a DFS briefing or stated that the assignee's supervisors or the assignee's co-workers were subject to interviews by DFS despite MD 12.3 requirements for these elements.

Plans are also inconsistent in the handling of proprietary and other sensitive unclassified information. For example, MD 12.3 requires information regarding protection of proprietary information to be documented in security plans. However, five of the 17 security plans reviewed did not specify that an assignee is not allowed to remove proprietary information from NRC despite MD 12.3 requirements.

Planning Not Transparent

Planning for the arrival of a foreign assignee is not transparent to the program offices. Some NRC managers cited poor matching of foreign assignee skills and interests to the work available in NRC program offices. Staff described ad hoc workarounds in these cases to make the assignments more beneficial for the assignee, but which also went outside the work and information descriptions in the security plans.

Inadequate Direction

Program offices do not always receive adequate direction from the Office of International Programs (OIP). Only two supervisors of foreign assignees of 14 interviewed cited information protection and only one cited the need to brief staff about security when discussing a supervisor's responsibility. In addition, other supervisors described relying on experience from different contexts, such as counterintelligence briefings for international travel, to guide them. More than half of supervisors interviewed did not receive or request a security briefing from DFS. NRC employees were not always told about foreign assignee access restrictions. Only a few supervisors of foreign assignees received a supervisory guide available from OIP. Supervisors cited the security plan as their primary guidance, even though the plans are not consistent and not intended to serve as guidance for supervisors or program office staff.

Why This Occurred

No Security Implementation Procedure

The security plan weaknesses occur because no specific procedure guides staff for consistent program implementation that would underpin

the security plan prepared for the assignee. The security plans are developed for each assignee from a template and are not intended to serve as a procedural document. The security plans are designed to inform the foreign assignee about what is permitted. They are intentionally vague to protect NRC's security program details and are inadequate guidance for NRC staff.

Why This Is Important

Program Offices May Not Maintain Effective Information Protection

Without adequate procedures, program offices may not be able to ensure effective information protection. When supervisors of foreign assignees rely on experience, the lack of procedures can result in an ad hoc approach. For example, a counterintelligence briefing preparing NRC staff for an international meeting would not cover the same issues as would a briefing to promote information protection while a foreign assignee is at NRC. In addition, previous experience with a foreign assignee may not be relevant in the circumstances of a different assignee, from a different country, or working on a different project. Program offices assume the risks of the foreign assignee program, sometimes without adequate guidance to manage them.

Recommendation

OIG recommends that the Executive Director for Operations and the Director, Office of International Programs

1. Develop a procedural document describing a consistent process for security planning, and for inviting, onboarding, and supervising foreign assignees to support information protection.

B. Foreign Assignee Use of External Email

Foreign assignees use a non-NRC, external email address while working at NRC, although agency policies rule out use of personal email. Foreign assignees do not have an NRC email address because that would require access to the internal local-area network and foreign assignees do not

meet the access standard to use NRC's network. The use of external email presents a potential risk of an unintentional spillage of information that should be protected.

What Is Required

Protecting Sensitive Information

NRC policies and rules are specific about protection of sensitive information. In particular, Management Directive (MD) 12.5 is NRC's policy for its Cybersecurity Program, including protecting information and IT systems from unauthorized access, use, disclosure, disruption, modification or destruction. MD 12.5 states that electronic transmissions shall not be automatically forwarded to non-NRC electronic destinations and sensitive information shall not be forwarded to personal (non-NRC) accounts. Also, MD 12.5 requires that foreign nationals that work at the NRC have a security plan that clearly defines computer security requirements that apply to their NRC assignments.

Further, NRC policy requires discretion in the transmission of Sensitive Unclassified Non Safeguards Information (SUNSI). The loss, misuse, or modification of, or unauthorized access to SUNSI can reasonably be foreseen as harmful to the public interest, to the conduct of NRC business, or to a commercial or financial interest to which the information pertains. Some types of SUNSI may be emailed within the NRC network. However, emailing SUNSI outside of NRC should be done as an exception when essential for the official conduct of NRC business. Some forms of SUNSI, including proprietary information, require encryption if emailed outside of NRC.

What We Found

Foreign assignees access a non-NRC, external email account using their NRC desktop computer and internet access. However, NRC does not know how the assignee uses the account, nor do NRC's security plans for foreign assignees mention or guide the use of email by foreign assignees.

Use of External Email

Foreign assignees use a personal email address or their email account associated with their foreign employer to communicate with NRC colleagues during their assignment. Interviews with supervisors of foreign assignees described ways NRC-related information could be transmitted between NRC staff and the assignees through external email accounts. Some assignees were provided NRC documents by email rather than hard copy. One assignee emailed their NRC-related work product using personal email to NRC's administrative support for printing when required.

Of the seven types of NRC information identified as SUNSI[1], proprietary information is the type foreign assignees are most likely to use, but assignees may be also be given access to certain sensitive internal information. Periodically, an assignee will be authorized to perform work involving security-related information.

None of the 17 security plans reviewed by OIG discussed appropriate use of email for foreign assignees. NRC does not monitor and cannot know whether emails in assignees' external accounts contain sensitive NRC information or other uses of the accounts. This is a concern even if classified or safeguards information is not being used.

Why This Occurred

NRC Email Not Available

Foreign assignees use external email accounts because NRC email is available only with access to the local-area network. Local-area network access is not allowed for foreign assignees, who do not meet the access standards for information security at NRC. NRC does not have the security controls or the infrastructure in place to grant foreign assignees secure access to any part of the local-area network. NRC's security plans all state that the foreign assignees will not have local-area network access.

[1] Seven types of SUNSI include allegation information; investigation information; security-related information; proprietary information; Privacy Act/Personally Identifiable Information; Federal-, State-, Foreign Government- and International Agency-Controlled Information; and sensitive internal information.

Why This Is Important

Potential for Information Spillage

Foreign assignee use of external personal or employer email accounts opens the potential for unintentional spillage of sensitive information. NRC is not able to mitigate weaknesses or detect improper use of the external email. Use of external email risks inadvertent transmissions of sensitive information.

Recommendations

OIG recommends that the Executive Director for Operations and the Director, Office of International Programs

2. Develop a secure, cost-efficient method to provide foreign assignees an email account which allows for NRC detection and mitigation of inadvertent transmission of sensitive information and seek Commission approval to implement it.

3. When an NRC approved email account is available, develop specific Computer Security Rules of Behavior for foreign assignees using the approved email.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations and the Director, Office of International Programs

1. Develop a procedural document describing a consistent process for security planning, and for inviting, onboarding, and supervising foreign assignees to support information protection.

2. Develop a secure, cost-efficient method to provide foreign assignees an email account which allows for NRC detection and mitigation of inadvertent transmission of sensitive information and seek Commission approval to implement it.

3. When an NRC approved email account is available, develop specific Computer Security Rules of Behavior for foreign assignees using the approved email.

V. AGENCY COMMENTS

An exit conference was held with the agency on December 14, 2016. Prior to this meeting, after reviewing a discussion draft, agency management provided comments that have been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess whether NRC's foreign assignee program provides adequate information security.

Scope

The scope of this audit included review of NRC activities surrounding foreign assignees who were present at NRC at any time from fiscal years 2014 to 2016. These 17 individuals provided an international cross section with an overview of recent experience and processes. OIG conducted this performance audit from July 2016 to October 2016 at NRC headquarters (Rockville, MD). Internal controls related to the audit objectives were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

OIG reviewed relevant laws, regulations, and policies. OIG conducted interviews of NRC staff and management and reviewed NRC documents pertaining to the foreign assignee program.

The documents reviewed include

- The Atomic Energy Act of 1954, as amended.
- Executive Order 13526, "Classified National Security Information".
- Title 10, Energy, Code of Federal Regulations, Section 810.
- U.S. Government Accountability *Office Standards for Internal Control in the Federal Government* (2014).
- NRC Management Directives:
    - 5.13, International Activities, Practices, and Procedures.
    - 12.1, NRC Facility Security Program.
    - 12.3, NRC Personnel Security Program.
    - 12.5, NRC Cybersecurity Program.

    - 12.6, NRC Sensitive Unclassified Information Security Program.
    - 12.7, NRC Safeguards Information Security.
- Security plans for foreign assignees.
- NRC bilateral agreements with the countries represented by the universe of assignees.
- NRC staff papers for the Commission.
- NRC office instructions and forms.

OIG interviewed NRC staff in the Office of International Programs, Office of the Chief Information Officer, Office of Administration, Office of Nuclear Security and Incident Response, Office of Nuclear Reactor Regulation, Office of Nuclear Material Safety and Safeguards, Office of Nuclear Regulatory Research, Office of New Reactors, Regions III and IV, and the Technical Training Center.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Beth Serepca, Team Leader; Amy Hardin, Audit Manager; Felicia Silver, Senior Auditor; and Ebaide Esoimeme, Auditor.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.