

50027

**General Information****Assigned Office:** ADM**OEDO Due Date:** 10/11/2013**Other Assignees:****SECY Due Date:****Date Response****Requested by Originator:** 10/11/2013**Other Parties:****Subject:** Audit of the Nuclear Regulatory Commission's Ongoing Eligibility for Access Authorization (OIG-13-A-22)**Description:****CC Routing:** NSIR, OCHCO, OGC, OIS**ADAMS Accession Numbers - Incoming:****Response / Package:****Other Information****Cross Reference No:** OIG-13-A-22**SRM\Other:** No**Process Information****Action Type:** Memo**OEDO Concurrence:** No**Signature Level:** DEDCM**OCM Concurrence:** No**Special Instructions:****OCA Concurrence:** No

Coordinate with OCHCO, OIS, NSIR and OGC, as appropriate. Please prepare response for the signature of DEDCM. Add Commission and SECY as cc's. Be sure to include the target completion date and identify the point-of-contact for each recommendation. Use attached instructions.

**Document Information****Originator Name:** Stephen D. Dingbaum**Date of Incoming:** 09/12/2013**Originator Org:** OIG**Document Received by OEDO Date:** 09/12/2013**Addressee:** Mark A. Satorius, OEDO**Incoming Task:** Memo**OEDO POC:**

Template: EDO-001

E-RIDS: EDO-01

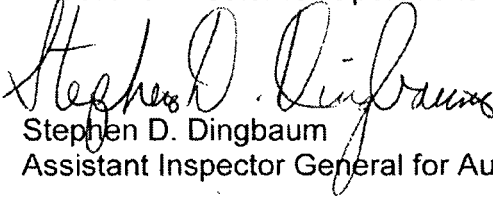


UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

OFFICE OF THE  
INSPECTOR GENERAL

September 12, 2013

MEMORANDUM TO: Mark A. Satorius  
Executive Director for Operations

FROM:   
Stephen D. Dingbaum  
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S ONGOING ELIGIBILITY FOR ACCESS  
AUTHORIZATION (OIG-13-A-22)

The Office of the Inspector General (OIG) conducted this audit to determine if the Nuclear Regulatory Commission (NRC) has processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility. OIG found that NRC employees rarely self-report the occurrence of certain events or conduct that may bring into question their reliability and trustworthiness even though such reporting is a requirement for continued NRC access authorization. Low-levels of self-reporting occur because NRC does not regularly inform employees of reporting responsibilities and there is no process to impose consequences for not self-reporting. OIG makes two recommendations to improve employee compliance with reporting responsibilities. Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

## **BACKGROUND**

The objective of NRC's personnel security program is to provide assurance that those with access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material<sup>1</sup> are reliable and trustworthy. In order to provide such assurance, NRC's Personnel Security Branch (PSB) administers the personnel security program, granting or denying access to classified information.<sup>2</sup> Additionally, PSB manages building access, information technology access, and access to safeguards information, and also administers NRC's drug testing program. For fiscal year 2013, the total resources budgeted to PSB were approximately \$2,855,000 and 14 full-time equivalent staff.

Access authorization is an administrative determination that an individual is eligible for a security clearance for access to Restricted Data<sup>3</sup> or National Security Information.<sup>4</sup> Access authorization eligibility requires an affirmative determination by PSB that the person in question is an acceptable security risk. The determination is a comprehensive, commonsense judgment, made after consideration of all the information, favorable or unfavorable, relevant to whether granting access authorization would be clearly consistent with the national interest.

A favorable determination results in PSB issuing a security clearance. Classified access requirements determine the type of clearance issued. All NRC employees are required to have a security clearance. PSB primarily issues the following clearances:

---

<sup>1</sup>Special nuclear material (SNM) is defined by Title I of the Atomic Energy Act of 1954 as plutonium, uranium-233, or uranium enriched in the isotopes uranium-233 or uranium-235. The definition includes any other material that the Commission determines to be SNM, but does not include source material. NRC has not declared any other material as SNM.

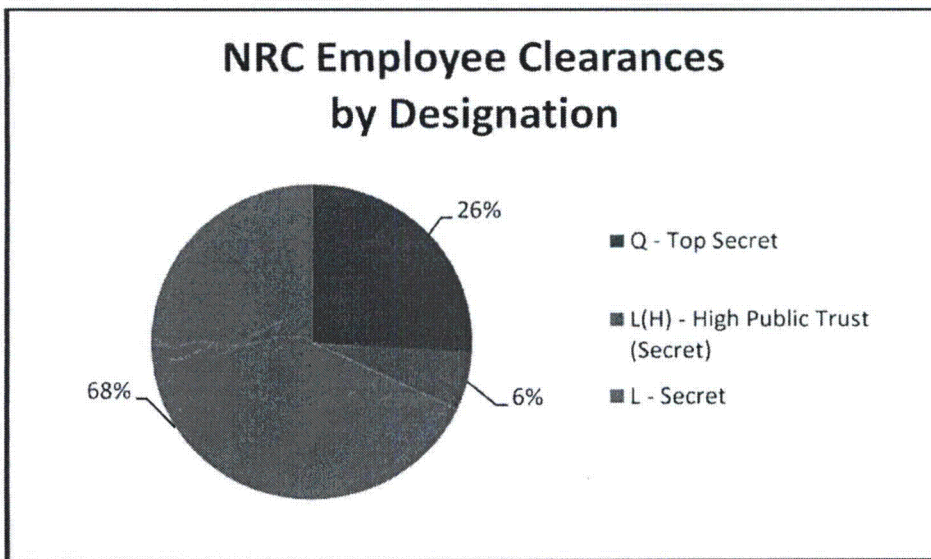
<sup>2</sup> The Office of Personnel Management (OPM) Federal Investigative Services Division is NRC's investigative provider. NRC applicants, employees, contractors, and licensees are submitted for investigation through OPM.

<sup>3</sup> Restricted Data: Information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.

<sup>4</sup> National Security Information: Information classified by an Executive Order, whose compromise would cause damage to the national security.

- Q Clearance – Top Secret  
This clearance authorizes access to the following information:<sup>5</sup>
  - ✓ Top Secret, Secret, and Confidential National Security Information.
  - ✓ Top Secret, Secret, and Confidential Restricted Data.
  
- L Clearance<sup>6</sup> – Secret  
This clearance authorizes access to the following information:<sup>5</sup>
  - ✓ Secret and Confidential National Security Information.
  - ✓ Confidential Restricted Data.

As of August 2013, 1,196 NRC employees had Q clearances, 3,146 had L clearances, and 296 were designated as L(H). The following chart illustrates the distribution of NRC employee clearances (percentages rounded):



Source: OIG generated

<sup>5</sup> An established need to know is also required.

<sup>6</sup> NRC also issues L(H) high public trust clearances. Classified access requirements for individuals with L and L(H) clearances are the same. However, individuals with L(H) clearances undergo a more rigorous initial background investigation and receive more frequent periodic reinvestigations.

Maintaining access authorization requires periodic background reinvestigations and adherence to security requirements. Individuals who possess "Q," "L(H)," or "L" security clearances undergo reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access authorization. PSB initiates a reinvestigation every 5 years for "Q" and "L(H)" (high public trust) clearances and every 10 years for "L" clearances. Additionally, individuals are required to self-report information to PSB that might compromise their continued eligibility for access to NRC facilities, material, or classified information.

### **OBJECTIVE**

The audit objective was to determine if NRC has processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility.

### **RESULTS**

NRC employees rarely comply with personnel reporting responsibilities for continued NRC access authorization. Reporting does not occur because NRC's existing processes are not sufficient to ensure compliance. Failing to comply with reporting requirements could result in national security being jeopardized.

### **Employees Not Complying with Personnel Reporting Responsibilities**

#### **Personnel Reporting Required**

NRC employees are required to comply with personnel reporting responsibilities for continued access authorization. NRC's Management Directive 12.3, *NRC Personnel Security Program*, requires employees to comply with a list of reporting responsibilities set forth in the directive. Specifically, employees are required to report certain events that may bring into question their reliability and trustworthiness. For example, the following are some of the events employees are required to report:

- Use of intoxicating beverages habitually to excess without evidence of rehabilitation.

- Use of, trafficking in, sale, transfer, or possession of an illegal drug or other controlled substance (except as prescribed by a physician licensed to dispense drugs in the practice of medicine), without evidence of rehabilitation.
- Arrests, charges, detentions, or any criminal conduct that indicates a history or pattern of criminal activity that creates doubt about a person's judgment, reliability, or trustworthiness.
- Any financial considerations that indicate an inability or an unwillingness to satisfy debts, and financial problems linked to gambling, drug abuse, alcoholism, or other issues of a security concern.

Additionally, Executive Order 12968<sup>7</sup> establishes a uniform Federal personnel security program for employees considered for initial or continued access to classified information. The order requires that employees who are granted eligibility for access to classified information comply with all security requirements and report violations of security regulations.

### **NRC Employees Rarely Comply with Personnel Reporting Responsibilities**

NRC employees rarely comply with personnel reporting responsibilities for continued access authorization. OIG reviewed a judgmentally selected sample of 35 NRC employee background reinvestigations to determine compliance with reporting responsibilities. The sample covered a period of approximately 20 months<sup>8</sup> and only included reinvestigations assigned an Issue Code<sup>9</sup> of B (moderate), C (substantial), or D (major).

---

<sup>7</sup> Executive Order 12968, *Access to Classified Information*, dated August 2, 1995.

<sup>8</sup> August 1, 2011, through April 19, 2013.

<sup>9</sup> OPM assigns an Issue Code to each investigation and reinvestigation. Issue Codes are used to identify concerns that may potentially disqualify a person from obtaining or maintaining access authorization.

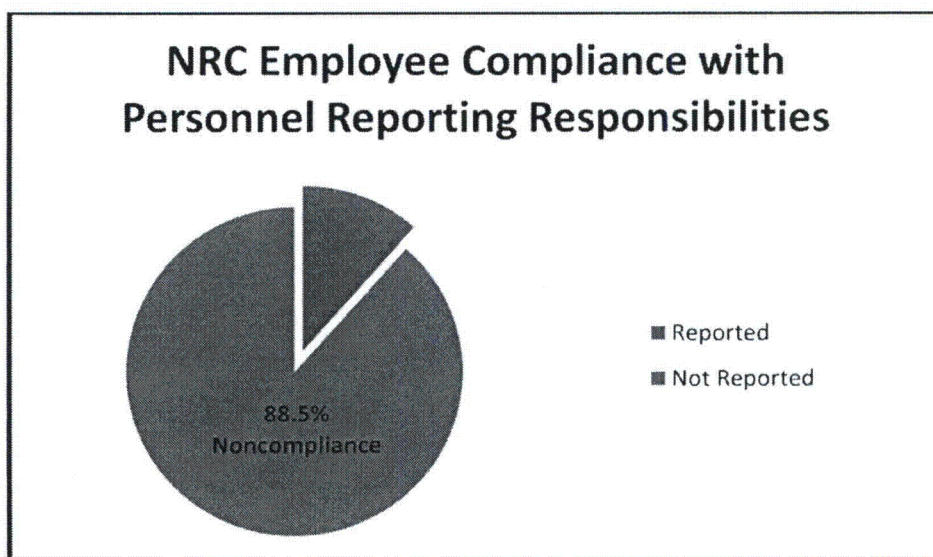


The results of OIG's review are summarized in the following table:

Issue Code	Employee Reinvestigation Files Reviewed	Files Containing a Reportable Event(s)	Files Containing an Event(s) Correctly Reported
B - Moderate	21	14	1
C - Substantial	7	6	1
D - Major	7	6	1
Totals	35	26	3

Reviewing the 35 reinvestigation files, OIG found 26 files containing information developed during the reinvestigation concerning certain events that might bring into question staff reliability and trustworthiness. These events should have been reported to PSB prior to the initiation of the reinvestigation. (The majority of the reportable events were financial in nature.) However, only 3 of 26 employees (approximately 11.5 percent) complied with personnel reporting responsibilities and reported to PSB as required by regulation.

The following chart graphically illustrates the results of the NRC employee reinvestigation file review (percentage rounded):



Source: OIG generated

## **NRC Does Not Have Sufficient Processes in Place To Ensure Compliance**

NRC does not have sufficient processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility. Specifically, NRC does not regularly inform employees of personnel reporting responsibilities and there is no process to impose consequences for not self-reporting.

### **NRC Employees Are Not Regularly Informed of Reporting Requirements**

NRC does not regularly inform employees of personnel reporting requirements for continued access authorization eligibility.

#### How NRC Employees Are Informed of Reporting Requirements

NRC initially informs new employees of personnel reporting requirements during the security briefing portion of new employee orientation.

NRC also recently issued two Yellow Announcements<sup>10</sup> via a "Daily Announcements" email informing employees of personnel reporting requirements. On October 5, 2012, NRC issued Yellow Announcement #127, listing specific events that require reporting to PSB. In response to employee questions, NRC issued Yellow Announcement #012 on January 23, 2013, clarifying Yellow Announcement #127 and providing a link to frequently asked questions on PSB's internal Web site. The questions generated by the issuance of the Yellow Announcement evidenced that NRC employees are not entirely familiar with personnel security reporting requirements. Prior to this recent effort, the last Yellow Announcement reiterating personnel reporting responsibilities was issued on April 9, 1999.

NRC issues many announcements. From January 2013 through July 2013, NRC issued 851 announcements (92 were Yellow Announcements). Earlier this year, NRC electronically sent out 11 announcements (4 of which were Yellow) to staff in one day. All announcements may not be read by all employees, especially on a day when 11

---

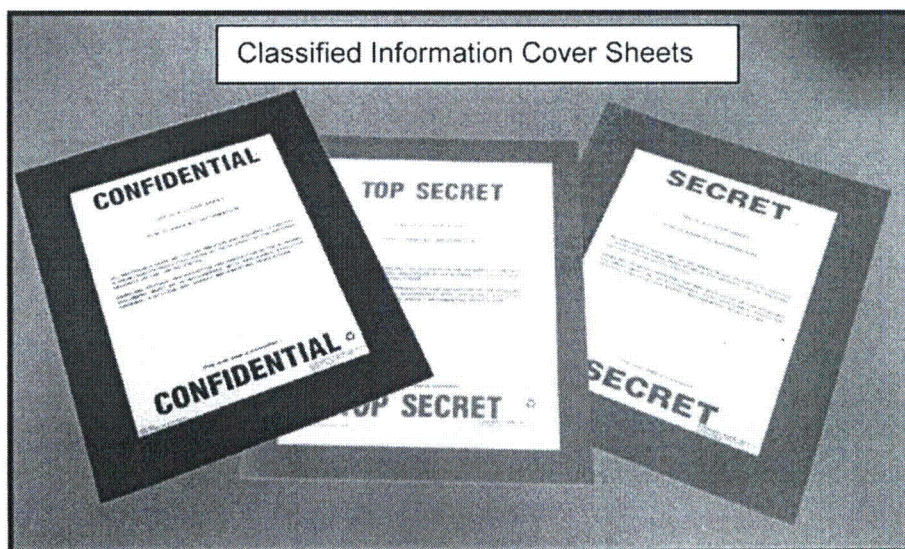
<sup>10</sup> NRC Yellow Announcements establish new policies, practices, or procedures; introduce changes in policy, senior staff and management assignments, or organization; or address major agencywide events. Announcements are posted to the agency intranet and are issued through the Office of Administration's NRC Announcement System.



announcements are communicated. Currently, NRC does not track whether employees are actually reading the announcements issued.

### Benchmark Comparison: How Department of Energy (DOE) Employees Are Informed of Reporting Requirements

Similar to NRC, DOE informs new employees of reporting requirements during a security briefing. However, unlike NRC, DOE headquarters employees possessing either a Q or L clearance are also required annually to take an online security briefing refresher course that reiterates the personnel reporting requirements. DOE tracks the required refresher training and strives to achieve a 100-percent completion rate. DOE Personnel Security Operations management confirmed that employees typically comply with reporting requirements.



Source: OIG

### **No Process To Impose Consequences for Not Self-Reporting**

There is no process to impose consequences for employees who fail to comply with personnel reporting responsibilities. Currently PSB staff may discuss self-reporting violations with the employee and note the conversation in the employee's file. However, without a defined mechanism to raise accountability and awareness, employees will continue not to self-report.

## **National Security Could Be Jeopardized**

Certain types of information must be assiduously protected. When a person's actions show evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on to protect classified information. The unauthorized disclosure of classified information can cause irreparable damage to the national security and loss of human life.

## **RECOMMENDATIONS**

OIG recommends that the Executive Director for Operations:

1. Develop and implement annual training that reinforces comprehension and confirms acceptance of NRC's personnel reporting requirements for continued access authorization eligibility.
2. Develop and implement a process that assigns consequences for individuals who do not comply with NRC's personnel reporting requirements for continued access authorization eligibility.

## **AGENCY COMMENTS**

An exit conference was held with the agency on September 11, 2013. Prior to this meeting, after reviewing a discussion draft, agency management provided supplemental information that has 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.

## **SCOPE AND METHODOLOGY**

We reviewed Federal and NRC guidance, Executive Orders, and relevant Government Accountability Office and OIG reports to develop criteria for this audit. To assess NRC's performance, we interviewed PSB management and staff to obtain their insight into the reinvestigation program and self-reporting requirements. Additional interviews were conducted with DOE Personnel Security Operations management to gain an understanding of their practices regarding self-reporting. We also reviewed a judgmentally selected sample of 35 NRC employee background reinvestigations to

determine compliance with reporting responsibilities. OIG conducted this audit at NRC headquarters (Rockville, Maryland) from February 2013 through July 2013. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program.

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.

This audit was conducted by Beth Serepca, Team Leader; Robert Woodward, Audit Manager; Larry Vaught, Senior Auditor; and Regina Revinzon, Student Intern.

## **Instructions for Responding to OIG Report Recommendations**

### **Instructions for Action Offices**

Action offices should provide a written response on each recommendation within 30 days of the date of the transmittal memorandum or letter accompanying the report. The concurrence or clearance of appropriate offices should be shown on the response. After the initial response, responses to subsequent OIG correspondence should be sent on a schedule agreed to with OIG.

Please ensure the response includes:

1. The report number and title, followed by each recommendation. List the recommendations by number, repeating its text verbatim.
2. A management decision for each recommendation indicating agreement or disagreement with the recommended action.
  - a. For agreement, include corrective actions taken or planned, and actual or target dates for completion.
  - b. For disagreement, include reasons for disagreement, and any alternative proposals for corrective action.
  - c. If questioned or unsupported costs are identified, state the amount that is determined to be disallowed and the plan to collect the disallowed funds.
  - d. If funds put to better use are identified, then state the amount that can be put to better use (if these amounts differ from OIG's, state the reasons).
3. An agency point-of-contact for each recommendation.

### **OIG Evaluation of Responses**

If OIG concurs with a response to a recommendation, it will (1) note that a management decision has been made, (2) identify the recommendation as resolved, and (3) track the action office's implementation measures until final action is accomplished and the recommendation is closed.

If OIG does not concur with the action office's proposed corrective action, or if the action office fails to respond to a recommendation or rejects it, OIG will identify the recommendation as unresolved (no management decision). OIG will attempt to resolve the disagreement at the action office level. However, if OIG determines that an impasse has been reached, it will refer the matter for adjudication to the Chairman.

### **Semiannual Report to Congress**

In accordance with the Inspector General Act of 1978, as amended, OIG is required to report to Congress semiannually on April 1 and October 1 of each year, (a) a summary of each OIG report issued for which no management decision was made during the previous 6-month period, and (b) significant recommendations from previous audit reports where final corrective action has not been completed. Heads of agencies are required to report to Congress on significant recommendations from previous OIG reports where final action has not been taken for more than 1 year from the date of management decision, together with an explanation of delays.