OFFICE OF
THE INSPECTOR GENERAL

U.S. NUCLEAR
REGULATORY COMMISSION

Review of NRC's Personnel Security
Program Contractor Policies and Practices

OIG-04-A-02 November 5, 2003

AUDIT REPORT

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

November 5, 2003

MEMORANDUM TO: William D. Travers

FROM: Stephen D. Dingbaum**/RA/**
Assistant Inspector General for Audits

SUBJECT: REVIEW OF NRC'S PERSONNEL SECURITY PROGRAM CONTRACTOR POLICIES AND PRACTICES (OIG-04-A-02)

Attached is the Office of the Inspector General's audit report titled, *Review of NRC's Personnel Security Program Contractor Policies and Practices.*

Auditors found that (1) NRC employees do not consistently implement the established contractor access policy and procedure requirements and (2) NRC does not act expeditiously to resolve access decisions pertaining to IT contractors when issues are reflected in the background investigation conducted by the Office of Personnel Management (OPM). Furthermore, because NRC does not screen OPM investigation results upon receipt to determine issue significance, cases that may warrant expedited resolution or immediate action cannot be identified for such treatment.

The report makes 10 recommendations to strengthen controls over the personnel security program with regard to contractor access to NRC headquarters and regional office facilities and information.

During an exit conference on September 26, 2003, NRC officials provided comments concerning the draft audit report. OIG incorporated these comments, as appropriate, into the report. NRC officials reviewed the modifications and opted not to submit formal written comments to this final version of the report.

If you have any questions, please contact Stephen D. Dingbaum, Assistant Inspector General for Audits, at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

cc: William Dean, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
B.J. Garrick, ACNW
M. Bonaca, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
E. Merschoff, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDH/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
J. Dyer, NRR
G. Caputo, OI
P. Bird, HR
C. Kelley, SBCR
M. Virgilio, NMSS
S. Collins, DEDR
A. Thadani, RES
P. Lohaus, STP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, NSIR
R. Wessman, IRO
H. Miller, RI
L. Reyes, RII
J. Caldwell, RIII
B. Mallett RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

EXECUTIVE SUMMARY

BACKGROUND

Most Nuclear Regulatory Commission (NRC) contractor employees are required to obtain approval through the agency's personnel security process prior to beginning work for the agency. Contractors receive one of three types of access: (1) classified access, which permits them to work with classified information; (2) information technology (IT) access, which permits them to work with NRC sensitive IT systems and information, and (3) building access, which allows them continuous unescorted access within headquarters or regional office facilities. Approval for access to these three levels is based on a background investigation conducted by the Office of Personnel Management (OPM) or the General Services Administration. Contractors are often granted temporary access before the background investigation is completed.

PURPOSE

The audit objectives were to determine (1) whether NRC policies for contractor employee access to agency information and facilities are being implemented and (2) whether the contractor temporary access process meets its goal of expediting contractor employment without jeopardizing NRC safety and security.

RESULTS IN BRIEF

Personnel security program weaknesses pertaining to contractor access to NRC headquarters and regional office facilities could be placing the agency's information, facilities, and staff at risk. Specifically, program requirements are not consistently followed and the agency lacks a process for expeditiously resolving final access decisions for IT contractors with temporary access when issues are reflected in the OPM background investigation.

Contractor Personnel Security Program Requirements Are Inconsistently Followed

NRC employees do not consistently implement the established contractor access policy and procedure requirements. OIG reviewed documentation and interviewed NRC project officers associated with 17 contracts and determined that contrary to NRC guidance and policy:

- Contractors were working prior to review and adjudication for temporary access by the Division of Facilities and Security (DFS).
- Contractors were escorting other contractors without approval to do so.
- Contractors with only building access had access to the NRC computer network.
- Contractors working offsite with sensitive information had not been approved for IT access.

- Security infractions were not consistently administered for contractor related security violations.

These lapses occur because NRC's personnel security program managers have not effectively documented or communicated contractor security policies to NRC staff expected to carry out these policies. As a result, some contractors are inappropriately given access to NRC facilities and data, potentially jeopardizing agency employees and information. In addition, DFS officials have made policy and procedure changes without formally documenting or providing rationale for those changes.

Agency Response to IT Temporary Access Issue Cases Is Not Timely

NRC does not act expeditiously to resolve access decisions pertaining to IT contractors when issues are reflected in the OPM background investigation. As of June 2003, DFS had a total of 80 investigative reports returned from OPM that needed to be reviewed and adjudicated for contractors already working at NRC with temporary access. Of these 80 reports, 70 had issues (i.e., questionable or derogatory background information of varying levels of significance), and 39 of these issue cases had been awaiting adjudication for 5 months or more. This slow response occurs because DFS lacks a process for resolving these cases quickly. Furthermore, because NRC does not screen OPM investigation results upon receipt to determine issue significance, cases that may warrant expedited resolution or immediate action cannot be identified for such treatment.

RECOMMENDATIONS

This report makes 10 recommendations to the Executive Director for Operations to strengthen controls over the personnel security program with regard to contractor access to NRC headquarters and regional office facilities. A consolidated list of recommendations appears on pages 21 – 22 of this report.

AGENCY COMMENTS

During an exit conference on September 26, 2003, NRC staff provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

ABBREVIATIONS AND ACRONYMS

CFR	Code of Federal Regulations
DFS	Division of Facilities and Security
FY	Fiscal Year
IT	information technology
LAN	local area network
MD	Management Directive
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OPM	Office of Personnel Management
SCIF	sensitive compartmentalized information facility

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

Government agencies are requesting more security clearances for Federal workers as part of the Nation's overall response to the terrorist attacks of September 11, 2001. In FY 2002, the Office of Personnel Management (OPM) — which manages the bulk of these requests — received almost 2 million requests for background investigations and other checks for contractors and employees. That was an increase of nearly 90 percent from the prior fiscal year. Background investigations serve as a basic protection against espionage or other misuse of classified and sensitive agency information, occupational fraud and abuse, and crime in the workplace. Due to a Governmentwide initiative to increase reliance on Federal contractor employees, the need for background investigations for these individuals will continue to grow.

One purpose of a personnel security background investigation is to determine whether past behavior is a matter of concern for future reliability. Background investigations vary in depth based on the type of work the employee or contractor will be doing. For example, Federal employees needing Confidential, Secret, and L clearances undergo an Access National Agency Check with Inquiries, while a Single-Scope Background Investigation is required for Top Secret and Q clearances.[1] Government employees who will not be working with classified information are required to undergo at least an investigation to assess their "suitability"[2] for Federal employment.

While the Office of the Inspector General (OIG) did not identify any regulations concerning suitability for contractors who will not be working with classified information, an OPM official explained that agencies are expected to hold these contractors to the same standard as Federal employees. Thus, agencies need to conduct background investigations appropriate to the level of risk posed by the contractor's access to agency facilities or information.

[1]To work with Confidential, Secret, or Top Secret classified information, individuals must receive at least the corresponding level of security clearance (i.e., Confidential, Secret, Top Secret). Pursuant to the Atomic Energy Act, NRC uses a separate system; employees either receive an L clearance, which equates to a Confidential or Secret clearance, or a Q clearance, which equates to a Top Secret clearance.

[2]According to Title 5, Part 731, Code of Federal Regulations (5 CFR Part 731), "*Suitability*," the determination of suitability for Federal employment is based on an individual's character or conduct that may have an impact on the integrity or efficiency of the service. These determinations of suitability for Federal employment are characterized in 5 CFR Part 731 as different than determinations of eligibility for assignment to sensitive national security positions.

NRC Contractor Security Requirements

In accordance with legislative requirements and agency policy, most contractor employees[3] working for the agency are required to undergo NRC's personnel security process prior to beginning work for NRC. Under these requirements, (1) contractors working with classified information or in positions of high public trust (e.g., security guard) must be approved for Q or L access authorization,[4] (2) contractors with access to NRC sensitive information technology (IT) systems and information must be approved for information systems access[5] (referred to in this report as IT access), and (3) contractors who require continuous unescorted access within headquarters or regional office facilities (but do not need IT access) must be approved for building access. Currently, there are approximately 960 contractors working for headquarters and regional office facilities. Approximately 90 have either Q or L access authorizations, while the remainder have either IT or building access.[6]

The Contractor Access Process

The process for granting IT and building access to contractors involves two phases: (1) a temporary access phase, which allows a contractor to begin work prior to a final access determination and (2) a final access phase, which is based on a more indepth background investigation. (See Appendix B for a flow chart depicting this process.) Each phase involves an evaluation — referred to as adjudication — of background information about the contractor employee. Division of Facilities and Security (DFS) staff adjudicate cases based on a set of guidelines used to assess individuals who work with classified information. DFS staff explained that when a contractor's background raises questions based on

[3]Contractors who will be working for 30 days or less at the headquarters or regional office facilities (e.g., pest control, specialty electrician) and do not need access to sensitive IT systems or data are not required to undergo a personnel security review. However, these contractors must be issued visitor badges on a daily basis and must be escorted by an NRC employee the entire time they are working in NRC facilities. In addition, contractors working offsite with non-sensitive NRC data are not currently required to undergo a personnel security review.

[4]The term access authorization is defined in Title 10, Part 10, Code of Federal Regulations (10 CFR Part 10), "*Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance,"* as an administrative determination that a prospective or current NRC employee or contractor is eligible for a security clearance for access to Restricted Data or National Security Information. For practical purposes, this term is interchangeable with "security clearance."

[5]The term access is not defined or even used in 10 CFR Part 10, but appears in NRC Management Directive and Handbook 12.3 (MD 12.3), "*NRC Personnel Security Program*," in connection with IT Level I, IT Level II, and building access contractors. Agency legal staff advised that the term access is not defined in 10 CFR Part 10 or MD 12.3, but is meant to convey the standard Webster's dictionary definition of the word (i.e., permission, liberty, or ability to enter, approach, communicate with, or pass to and from).

[6]DFS could not easily provide a breakdown of contractors with IT access versus building access.

the guidelines, such questions are referred to as *issues*. The staff will attempt to resolve — or mitigate — these issues by considering, for example, when the problems occurred, their seriousness, and if they have been or are being resolved.

During the temporary access phase, DFS staff review written personnel security background information provided by the prospective contractor and credit and criminal histories for these individuals. Based on the staff's adjudication of this information, a DFS branch chief grants (or denies) temporary access allowing the contractor to begin work, unescorted, in the headquarters or regional office.

The second phase of NRC's security process occurs following the approval for temporary access. In this phase, DFS requests from either OPM (for IT access) or the General Services Administration (for building access) a more comprehensive background investigation. When these background investigation results are returned (several months to more than a year after the request is made), DFS staff review and adjudicate the information. Based on this second review, the DFS Security Branch Chief makes a determination to either grant or deny final access to these contractors.

NRC Guidelines for Determining Eligibility for Access

Guidelines used by DFS staff to assess contractors for temporary and final access approval appear in Title 10, Part 10, Code of Federal Regulations (10 CFR Part 10), "*Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance*." These guidelines assess the individual's loyalty to the United States and whether he or she could be susceptible to pressure to act against the interests of national security. Items to be assessed include whether the individual:

- Has a history of financial problems.
- Provided false information on the personnel security questionnaire.
- Uses alcohol excessively.
- Uses illegal narcotics.
- Has a background suggesting criminal tendencies, poor judgment, unreliableness, or untrustworthiness.
- Knowingly established or continued a sympathetic association with a representative for a foreign nation whose interests may be contrary to the interests of the U.S.

Recent DFS Efforts To Improve Controls

DFS staff and managers described various efforts made over the past several years to improve controls over contractor access to NRC facilities and information. These efforts included issuing several memoranda from the Office of Administration to office directors urging compliance with agency access

requirements, presenting a security segment in NRC's project officer training, issuing security infractions to project officers who violate the MD requirements, and meeting with project officers and their managers to discuss concerns relating to contractor access. According to the DFS Director, these efforts have caused a significant reduction in the number of contractors working in the headquarters buildings on an escorted basis without prior security review. Furthermore, he noted, there has been no recent evidence of theft or compromise of information related to contractors.

II. PURPOSE

The audit objectives were to determine (1) whether NRC policies for contractor employee access to information and facilities are being implemented and (2) whether the contractor temporary access process meets its goal of expediting contractor employment without jeopardizing NRC safety and security. These objectives were derived as part of OIG's overall review of the efficiency and effectiveness of NRC's personnel security program, which is still in process.

III. FINDINGS

Personnel security program weaknesses pertaining to contractor access to NRC headquarters and regional office facilities could be placing the agency's information, facilities, and staff at risk. Specifically, program requirements are not consistently followed and the agency lacks a process for expeditiously resolving final access decisions for IT contractors with temporary access when issues are reflected in the OPM background investigation.

A. CONTRACTOR PERSONNEL SECURITY PROGRAM REQUIREMENTS ARE INCONSISTENTLY FOLLOWED

NRC employees do not consistently implement the established contractor access policy and procedure requirements. OIG reviewed documentation and interviewed NRC project officers associated with 17 contracts and determined that contrary to NRC guidance and policy:

- Contractors were working prior to review and adjudication for temporary access by DFS.
- Contractors were escorting other contractors without approval to do so.
- Contractors with only building access had LAN[7] accounts.
- Contractors who had not been approved for access were working offsite with sensitive information.
- Security infractions were not consistently administered for contractor related security violations.

These lapses occur because NRC's personnel security program managers have not effectively documented or communicated policies concerning contractors to NRC staff expected to carry out these policies. As a result, some contractors are inappropriately given access to NRC facilities and data, potentially jeopardizing agency employees and information. In addition, DFS officials have made policy and procedure changes without formally documenting or providing rationale for those changes.

NRC Policy and Procedures

NRC has established policy and other requirements to protect information, staff, and facilities in accordance with laws, Executive orders, and management directives. Management Directive and Handbook (MD) 12.3, "*NRC Personnel Security Program*," contains the policies and procedures establishing a personnel security program to ensure that determinations of an individual's

[7] The Local Area Network (LAN) is a group of computers connected together to share information and hardware in a small area.

eligibility for access to information and facilities are in accordance with pertinent laws and other guidance. While some requirements are formalized as policy in NRC management directives, others are not. DFS officials convey NRC personnel security program requirements not formalized in the MDs through various means, such as Yellow Announcements, the NRC Web site, and through discussion. These policies and requirements address a number of topics, including when contractors may begin working for the agency, contractor escorting requirements, temporary access process steps, DFS's review of contract security clauses, and the use of NRC's security infraction program to address noncompliance with requirements.

Contractor Security Policies Not Well Documented or Communicated

NRC employees do not consistently follow the established contractor access policy and procedure requirements because these requirements are not well communicated to staff in written policy or via other means. As a result, some contractors are inappropriately given access to NRC facilities and data, placing agency employees and information at risk. In addition, DFS officials have made policy and procedure changes without formally documenting or providing rationale for those changes.

OIG reviewed documentation and interviewed NRC project officers associated with 17 contracts and identified 5 types of inconsistencies between policy and practice on 7 of the contracts. No single contract reviewed demonstrated all five inconsistencies, but some served to illustrate as many as three. The following are examples of inconsistencies identified.

Contractors Working Prior to DFS Approval

NRC allows contractors to begin working for NRC once they are approved by DFS. However, 14 contractors working on 4 of the contracts reviewed by OIG had worked prior to or without DFS review and adjudication for temporary access. One example involved a health center contract employee who was inappropriately signed in as a visitor for approximately 6 weeks. In this case, the NRC project officer had submitted the paperwork to DFS, but such approval had not yet been granted. The project officer explained that he allowed the contractor to come on board prior to DFS approval because he did not want to lose the opportunity to employ this individual, whom he felt was highly qualified for the position.

Another example involved contractors working at headquarters to construct a sensitive compartmentalized information facility (SCIF) for storing and discussing classified information. Nine of 10 construction contractors or subcontractors were signed in as visitors to work on the SCIF project. One of these individuals, who worked for 9 days at NRC without having received approval, was then denied access approval because of financial-related criminal conduct in his

background. Moreover, approximately 2 months after another proposed contractor employee was denied access approval due to a violent criminal background, the NRC project officer — who had been informed in writing that this individual was not to have access to NRC facilities or information — resubmitted the employee's name for weekend access.[8] In this circumstance, a DFS official recognized the individual's name and, consequently, the request was denied.

The DFS Director told OIG that he gave his approval for the SCIF project contractor employees to be signed in as visitors to work prior to their adjudication for temporary access because he believed it necessary to expedite work on the project. He said he conveyed his approval for the visitor sign-ins verbally to the NRC project officer for the contract, but did not formally document the decision.

Contractors Escorting Other Contractors Without Approval

NRC requires agency employees to escort short-term contractor employees who are not required to obtain access approval. However, on three contracts, contractors who did not have permission escorted at least four such contractors. The NRC project officers for two of the contracts said they work in offices situated apart from the areas in which the contractors worked and were unaware that these violations were occurring. On the third contract, the project officer, who also worked in an area removed from the contractor work area, explained that the foreman of the crew had building access approval and could be trusted to supervise the other contractors. This project officer explained that it would be inconvenient for NRC staff to have to perform all of the escorting.

Although DFS staff occasionally approve contractors to escort other contractors, this option is not documented in MD 12.3. There are no criteria for who may grant the approval, what qualifications the contractor should possess in order to escort, or under what circumstances this permission is granted. Until recently, DFS did not have a single, up-to-date list of contractors who had been granted escort permission.

Building Access Contractors With LAN Accounts

NRC requires IT access for contractors to have NRC LAN accounts. Yet, OIG identified 10 contractors with only building access (working on three contracts) who had LAN accounts. Project officers for these contracts were not aware that this practice was prohibited.

[8]While the project officer was advised that the contractor was not permitted to work on the SCIF project, the project officer was not informed of the specific reason for the denial of access.

MD 12.3 states that IT access is needed for access to NRC sensitive IT systems and data, but does not specifically mention assignment of LAN accounts. DFS staff explained that contractors should not have a LAN account unless they have been approved for IT access. While some project officers were aware of this requirement, others were not. According to DFS managers, they have made concerted efforts to communicate the requirements for contractor LAN access to agency staff and to Office of the Chief Information Officer (OCIO) staff in particular. They said the situation has improved due to these efforts and explained that a revised version of Management Directive 12.5, "*NRC Automated Information Systems Security Program*," incorporates procedures clarifying that OCIO will not grant contractors LAN access until receiving verification from DFS that the appropriate security clearance or IT access had been granted.

Contractors Working Offsite With Sensitive Information

According to DFS staff, contractors working offsite with sensitive information are required to be approved for IT access. However, three employees working offsite on two contracts did not have IT access approval. In one case, an offsite contractor employee who was working with sensitive information did not have IT access approval. In another case, an offsite contractor employee who was supervising onsite contractor employees did not have IT access approval. Yet, the work performed by the onsite staff required them to have IT access. While the NRC project officer said the offsite supervisor was not working with systems information, but was overseeing the contract, the scenario causes OIG to question the offsite supervisor's access to sensitive NRC information.

The requirement for contractors working offsite with sensitive information is not clearly stated in MD 12.3. MD 12.3 discusses "access to NRC sensitive information technology systems and data by NRC contractors," but does not clearly state that sensitive data covers more than IT information. As one DFS official explained, such access approval is required in cases where a breach of the information protection requirements could have safety and security implications.

Security Infractions Not Consistently Administered

Security infractions are used to address some types of noncompliance with personnel security requirements,[9] however, security infractions are not issued consistently for policy and procedure violations. For example, the project officer for the SCIF construction effort was not given an infraction after permitting contractors to begin work prior to review and adjudication for temporary access.

[9] A security infraction is an administrative action that DFS takes when an employee fails to comply with NRC security requirements. DFS staff advised that if an employee receives three security infractions within a year, they can lose their security clearance and, consequently, their job at NRC.

Instead, the project officer was given permission by the DFS Director to allow the employees to work prior to approval for project expediency purposes. However, the project officer for a different contract was given a security infraction for the same practice. The DFS Director told OIG he does not view the SCIF scenario as warranting an infraction because he approved the contractors to begin work prior to DFS review and adjudication and he has the authority to make these types of decisions. The option for project officers to request exemptions to DFS procedures is not documented in MD 12.3.

Moreover, neither NRC's contractor security requirements nor the fact that one can receive a security infraction for violating these requirements are clearly communicated to staff. As evidenced in the above examples, key guidance in MD 12.3 is unclear or incomplete. While a DFS staff member has been providing security training for approximately 1½ years to participants in the agency's project officer training courses, the training was not provided during all of the sessions conducted during this time period.

Policy and Procedure Changes Not Always Documented

DFS management officials have made policy and procedure changes without formally documenting or providing rationale for those changes. In one example, a DFS manager instructed adjudicators to stop conducting security assurance interviews that are required by MD 12.3 as a precursor to granting temporary access. The DFS manager advised that routinely holding security assurance interviews with prospective contractor employees was not likely to add value to the temporary access process. This manager said that if a prospective contractor answered questions dishonestly on their security forms, it was unlikely that they would tell the truth during an interview. The manager said that a face-to-face interview would be useful only if DFS staff had documentation proving that the contractors' written answers were inaccurate and that such information was not available during the temporary access phase.

In contrast, a personnel security official from another Federal agency acknowledged the benefits of conducting security interviews in situations where the contractor would be working with sensitive information. This official said the body language and other cues that are seen in a face-to-face interview are highly informative and could help to reveal inaccuracies on a security questionnaire. The official said a decision to conduct this type of interview ought to be based on the potential harm that could be caused by a contractor based on the type of work they would perform and their exposure to sensitive information. In addition, information developed during this initial interview could be extremely useful to reference if issues develop during the background investigation.

In a second example, a DFS manager instructed the DFS staff to stop evaluating the financial information of contractors when determining their eligibility for building access. Reviewing the credit report information for prospective building access contractors was intended to strengthen the background review performed on these contractors. In this case, the DFS manager explained that the requirement was preventing too many contractors from being approved. This manager said that many of these individuals had credit problems of varying degrees, and could not be approved to begin work. The manager told OIG that, in fact, it was never intended that the adjudicators use the financial information in the credit report for adjudicating contractors for building access. Rather, they were expected to use the report only to determine whether fraud alerts are reflected on the report or if there are discrepancies in the social security number, address, or name of the applicant that might suggest fraud. Therefore, the manager instructed staff to stop reviewing the financial information, and to review the credit report only for indicators of fraud. Again, this change was not documented.

By making informal policy changes without documenting those changes, NRC increases the risk of missing valuable information during its access approval process.

Fraud Examiners Advocate Strong Internal Controls, Background Investigations

In its *2002 Report to the Nation on Occupational Fraud and Abuse*, the Association of Certified Fraud Examiners presents results of a survey it conducted of approximately 10,000 certified fraud examiners in the United States. As part of the survey, respondents were asked, based on their own expertise, which of eight measures were most helpful in preventing fraud against organizations. Respondents reported that the top two most effective anti-fraud measures were, first, a strong system of internal controls, and second, detailed background checks on new employees.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Update and clarify MD 12.3 to reflect agency requirements concerning contractors working prior to approval, contractor escort requirements, level of access required to have a LAN account, and contractors working offsite with sensitive information.

2. Specify in MD 12.3 examples of violations that could warrant a security infraction and administer the security infraction program consistently in accordance with these rules.

3. Consistently provide materials on personnel security requirements in the project officer training course.

4. Develop and implement a plan to communicate on a routine basis directly with all NRC project officers concerning contractor security requirements. The plan should include such elements as mandatory annual refresher training on security requirements for all project officers and e-mail reminders to all project officers concerning the requirements.

5. Develop and implement a formal process for granting and documenting exceptions to security requirements and identify who is authorized to grant such exceptions.

6. Broaden the use of the credit report information for building access contractors so that information pertaining to financial issues is considered during the adjudication process.

B. AGENCY RESPONSE TO IT TEMPORARY ACCESS ISSUE CASES IS NOT TIMELY

NRC lacks a process for expeditiously resolving final access decisions for IT contractors with temporary access when issues are reflected in the OPM background investigation. This slow response occurs because DFS lacks a process for resolving these cases quickly. NRC emphasizes granting temporary IT access as quickly as possible, while delaying action on final access review, thus permitting contractors with questionable backgrounds to continue working until a final adjudication is made. Furthermore, because NRC does not screen OPM investigation results upon receipt for the significance of the issues that OPM identified, cases that may warrant expedited resolution or immediate action cannot be identified for such treatment. As a result, contractor employees with questionable backgrounds could be permitted to work at NRC, potentially jeopardizing the safety and security of agency employees and information.

Temporary Access Requirements

The purpose of NRC's temporary access program for contractors is not stated in policy, but the program is presumably intended to bring contractors on board quickly without jeopardizing NRC workplace safety or security.

MD 12.3 states that NRC must follow due process procedures if it seeks to deny final access to a contractor who has been allowed temporary IT access. (There is no due process requirement for denying access to building access contractors.) MD 12.3 also states, "On the basis of DFS's review of the contractor employee's security forms and/or the receipt of adverse information, the contractor employee may be denied access to NRC sensitive information technology systems and data until a final determination of eligibility for access is made under the provisions of due process." MD 12.3 does not state which DFS

official is responsible for making this decision to deny access pending due process procedures.

Due process requirements for IT contractors are not described in the Code of Federal Regulations. While 10 CFR Part 10 requires due process procedures in connection with suspension or revocation of "access authorization" (i.e., security clearances), the regulations do not address either the subject of "access" or "temporary access." Therefore, the due process requirements for revoking temporary access stem from MD 12.3 and are not directed by a higher regulatory or legislative source.

Issue Case Resolution is Untimely

Review of DFS's backlog of OPM investigation results found that NRC's personnel security program fails to deal with IT contractor "issue" cases in a timely manner.

As of June 2003, DFS had a total of 224 OPM reports that needed review and adjudication for employees and contractors. Of the 224, 80 were for contractors already working at NRC with temporary access. Of these 80 OPM reports, 70 had issues, and 39 of these issue cases had been awaiting adjudication for 5 months or more.[10] (See table for more details.)

IT Contractor Issue Cases Awaiting Final Access Determination by NRC	
Time since case returned from OPM	**Number of cases**
0 to 1 months	6
1 to 2 months	11
2 to 3 months	7
3 to 4 months	7
5 months to 1 year	28
1 year to 2 years	10
Over 2 years	1
Total	70

[10] 5 CFR Part 732, "*National Security Positions*," which pertains to Federal employees in national security positions, requires agencies to adjudicate background investigation results and report to OPM on those results within 90 days of receiving the background investigation report. This provides a guide as to acceptable/reasonable time frames for review.

DFS staff explained that their priority is to get prospective NRC staff and contractors approved for temporary access or access authorization as quickly as possible so these individuals can begin working, rather than deal with issue cases promptly. A DFS manager explained that while it would be desirable to deal with issue cases sooner, this is not possible given the staff's workload, the considerable amount of overtime the staff already work on a regular basis, and the demand by program offices to bring employees and contractors on board quickly. DFS staff members commented that the number of special requests they receive to expedite certain cases and other special projects that periodically arise make it impossible to deal with cases in a first-come, first-served manner. They also explained that most OPM investigation results contain issues concerning those investigated, but that in hindsight they find that the majority of issues are minor and, ultimately, mitigated so that final access can be granted.

DFS staff also perceive that there is no quick way to revoke a contractor's access when derogatory information arises. They said this is because of the agency's requirement that revocation of access cannot be made without undergoing required due process procedures. One staff member explained that there is no difference in the due process requirements afforded to IT contractors during either the temporary or final access phase. According to the staff member, preparing the evidence to support these cases is extremely time-consuming and labor-intensive. Another staff member explained that this evidence needs to be discussed with the Office of the General Counsel (OGC), which determines whether NRC can go forward with the case based on the evidence. If OGC does not believe the case is supported, DFS will not go forward with the case, the staff member explained. (As stated previously, due process procedures for IT contractors are not required by NRC regulations, but are established at the management directive level.)

Process Is Inadequate

This slow response to adjudicate contractor issue cases occurs because DFS lacks a process for addressing and resolving these cases promptly.

Office of Administration goals for personnel security emphasize quantity of case resolution (i.e., FY 03 performance measure to complete adjudication of 702 security investigations/ reinvestigations) over the more time consuming aspects of the personnel security process such as reviewing and resolving cases with issues. Staff work priorities follow suit. For example, DFS staff strive to meet an unwritten timeliness goal for reviewing and adjudicating requests for temporary access (1 to 2 weeks to complete their review once paperwork submitted is complete) for IT and building access contractors. However, they do not have a timeliness goal for reviewing and adjudicating the information that is returned from OPM in order to make a decision concerning final access.

Furthermore, there is no requirement that issue cases receive an initial screening to determine the level of risk to the agency that could result from allowing the contractor to have continued access. DFS staff members said they try to review the OPM results within a few days of receipt to see whether OPM has flagged the case as significant. They also said that sometimes they purposely look for OPM's response if it pertains to a troublesome case. However, as part of any initial review, they do not routinely compare the OPM results to the information used to grant temporary access to determine, for example, whether there are significant discrepancies. That type of in-depth review is not made until the DFS staff member decides to focus on a particular issue case in their backlog in order to close the case.

While DFS staff members said they inform their manager about their workload every 2 weeks, DFS management does not routinely track issue cases from receipt to resolution.[11] Staff members do not routinely report to the manager about all pending issue cases, but only those on which they are currently working or have resolved.

The due process requirements for IT contractors — which are perceived by DFS staff as time consuming and burdensome — are not required by NRC regulations. Therefore, NRC's policy could be modified to one that resolves issue cases with fewer resources. For example, at the U.S. Department of State, if employment offers are made prior to completion of the full investigation, the offers are conditional and contingent on a positive investigation outcome.

Security Risk Unaddressed

By failing to screen or review issue cases in a timely manner, NRC potentially allows individuals who may be a security risk to the agency to maintain access to agency facilities and information. Permitting the cases to remain unaddressed for months serves, in a sense, as a defacto adjudication without review. NRC can better protect its information, facilities, and employees by developing a process to treat issue cases (particularly those which are significant) as priorities and by adjusting policies that serve as obstacles to timeliness.

Recommendations

OIG recommends that the Executive Director for Operations:

7. Develop performance measures that assess the timeliness of DFS's adjudication of all cases back from OPM and issue cases in particular.

[11] Staff inform the manager about the number of cases they are currently working on and the number of cases closed.

8. Screen contractor cases returned from the Office of Personnel Management upon receipt for significance of issues raised and adjudicate those with significant issues on a priority basis.

9. Deny access to contractors with significant issues unless and until the case is resolved in the contractor's favor.

10. Incorporate clauses into NRC contracts specifying that temporary IT access approval for contract employees may be revoked immediately if issues surface during the background investigation that call into question the contractor's suitability for employment at the agency.

[Page intentionally left blank.]

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Update and clarify MD 12.3 to reflect agency requirements concerning contractors working prior to approval, contractor escort requirements, level of access required to have a LAN account, and contractors working offsite with sensitive information.

2. Specify in MD 12.3 examples of violations that could warrant a security infraction and administer the security infraction program consistently in accordance with these rules.

3. Consistently provide materials on personnel security requirements in the project officer training course.

4. Develop and implement a plan to communicate on a routine basis directly with all NRC project officers concerning contractor security requirements. The plan should include such elements as mandatory annual refresher training on security requirements for all project officers and e-mail reminders to all project officers concerning the requirements.

5. Develop and implement a formal process for granting and documenting exceptions to security requirements and identify who is authorized to grant such exceptions.

6. Broaden the use of the credit report information for building access contractors so that information pertaining to financial issues is considered during the adjudication process.

7. Develop performance measures that assess the timeliness of DFS's adjudication of all cases back from OPM and issue cases in particular.

8. Screen contractor cases returned from the Office of Personnel Management upon receipt for significance of issues raised and adjudicate those with significant issues on a priority basis.

9. Deny access to contractors with significant issues unless and until the case is resolved in the contractor's favor.

10. Incorporate clauses into NRC contracts specifying that temporary IT access approval for contract employees may be revoked immediately if issues surface during the background investigation that call into question the contractor's suitability for employment at the agency.

[Page intentionally left blank.]

V. AGENCY COMMENTS

During an exit conference on September 26, 2003, NRC staff provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

[Page intentionally left blank.]

Appendix A

SCOPE AND METHODOLOGY

This audit reviewed U.S. Nuclear Regulatory Commission (NRC) contractor access policies and practices to determine (1) whether NRC policies for contractor employee access to information and facilities are being implemented and (2) whether the contractor temporary access process meets its goal of expediting contractor employment without jeopardizing NRC safety and security. The audit focused specifically on Information Technology (IT) Level I, IT Level II, and building access contractors working in NRC headquarters and regional office facilities. This audit was performed as part of an overall, ongoing, review of NRC's personnel security program.

The Office of the Inspector General (OIG) audit team reviewed relevant criteria such as The Atomic Energy Act of 1954; Title 10, Part 10, of the Code of Federal Regulations, "Criteria and procedures for determining eligibility for access to restricted data or national security information or an employment clearance"; Executive Order 12968, "*Access to Classified Information*"; Management Directive and Handbook (MD) 11.1, "*Acquisition of Supplies and Services*"; MD 12.3, "*NRC Personnel Security Program*"; and other agency and Federal documents.

Auditors interviewed staff in the Division of Facilities and Security (DFS) to better understand the process for granting temporary access and denying final access to IT Level I, IT Level II, and building access contractors; an attorney in the Office of the General Counsel to better understand the agency's due process requirements for denying final access to IT contractors who were previously granted temporary access; and NRC project officers to determine if contractor policies were implemented in accordance with requirements. Auditors also reviewed the GroupWise address book to determine whether contractors with building access had been assigned LAN accounts. In addition, auditors reviewed personnel security case files for IT contractors to quantify the backlog of cases with issues that are awaiting adjudication for final access by NRC.

This work was conducted from January 2003 through June 2003, in accordance with generally accepted Government auditing standards and included a review of management controls related to audit objectives. The work was conducted by Vicki Foster, Senior Management Analyst; Judy Gordon, Senior Management Analyst; Beth Serepca, Team Leader; and Rebecca Underhill, Management Analyst.

[Page intentionally left blank.]

Appendix B

CONTRACTOR ACCESS APPROVAL PROCESS