January 23, 2007

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S BADGE ACCESS SYSTEM
(OIG-07-A-10)

Attached is the Office of the Inspector General's (OIG) report titled, *Audit of NRC's Badge Access System.*

This report presents the results of the subject audit. Agency comments provided at the exit conference on December 19, 2006, have been incorporated, as appropriate, into this report. The agency did not provide formal comments.

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 follow up 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 415-5915, or Beth Serepca at 415-5911.

Attachment: As stated

ELECTRONIC DISTRIBUTION

Frank P. Gillespie, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Luis A. Reyes, Executive Director for Operations
Janice Dunn Lee, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration and Chief Information Officer, OEDO
Michael R. Johnson, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
R. William Borchardt, Director, Office of New Reactors
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

AUDIT REPORT

Audit of NRC's Badge Access System

OIG-07-A-10 January 23, 2007

I. EXECUTIVE SUMMARY

BACKGROUND

The Nuclear Regulatory Commission's (NRC) automated badging and card reader system is an important component of the agency's physical security program. NRC uses the system to manufacture photo-identification badges for employees, contractors, and visitors and control their access within NRC's headquarters, regional offices, and the Technical Training Center (TTC). NRC refers to its system as the Access Control and Computer Enhanced Security System/Photo Identification Computer System (ACCESS/PICS). In this report, the system is referred to as ACCESS, and NRC regional offices and TTC are referred to as field offices.

PURPOSE

The objective of this audit was to determine whether the current badge access system meets its required operational capabilities and provides for the security, availability, and integrity of the system data.

RESULTS IN BRIEF

NRC's badge access system is capable of providing effective support for NRC's physical security program. However, specific cost-effective actions are needed to enhance this legacy system's usage at NRC until a replacement system is implemented. Auditors identified the following shortcomings with regard to ACCESS and related badge accountability processes:

- Weaknesses exist concerning system user access.
- The system contains inaccurate data.
- Badge accountability measures are inadequate.
- System documentation is incomplete or missing.
- TTC lacks a backup power supply for ACCESS.

These problems exist because concerns about ACCESS are overshadowed by the agency's plan to replace the system as part of its Homeland Security Presidential Directive -12 (HSPD-12) solution. Left unaddressed, these weaknesses undermine the effectiveness of NRC's physical security approach to control access into and within NRC facilities.

Weaknesses Exist Concerning User Access

ACCESS does not fully employ required user access controls. Specifically, in headquarters and a field office, several people share one user identifier (ID), 2 of 11 headquarters users have inappropriate access to the system, and a majority of the headquarters users have been granted the highest level of system access. Noncompliance with agency requirements has occurred because there is no routine review of the user access, limitations exist with one site's version of ACCESS, and NRC staff cannot easily define or differentiate the difference among ACCESS user roles. Without adequate user access controls, security information is vulnerable to errors or misuse.

System Contains Inaccurate Data

ACCESS contains inaccurate data pertaining to special access areas and the current employee population. These data inaccuracies exist because NRC does not impose effective quality assurance measures over access lists or system data. Without accurate information, there is the possibility of security breaches and ineffective control over special access areas.

Badge Accountability Measures Are Inadequate

NRC lacks adequate control over temporary badges issued to staff and visitors, and over badges issued to contractors. Specifically,

- Temporary badges loaned to staff who forget or lose their badge are not always returned the day they were issued.
- Temporary visitor badges are not inventoried and accounted for on a daily basis at headquarters and three field office sites.
- Contractor badges are not always retrieved promptly or deactivated once it is determined a particular contractor is no longer working for NRC.

Temporary and contractor badges are not always returned promptly because the agency has not asserted measures to enforce these requirements. Daily reconciliation of visitor badges is not performed at headquarters or several NRC field offices because NRC has not enforced this requirement. These weaknesses increase NRC's risk that temporary and contractor badges will be misused to gain unauthorized access into NRC facilities.

System Documentation Is Incomplete or Missing

NRC has not adhered to agency listed system security requirements for ACCESS or followed up on penetration testing results. This is because the agency has not viewed fulfillment of these requirements as a priority given that (1) ACCESS is a legacy system unlikely to attain certification and accreditation[1] and (2) a Government-wide interoperable solution is expected to replace ACCESS in FY 2009. Without following security requirements, NRC has limited assurance that ACCESS is adequately protected against unauthorized access or other misuse. In addition, ACCESS system owners and users are unable to locate relevant information when needed.

TTC Lacks Backup Power Supply

TTC's card reader contingency plan in the event of a power failure is workable, but causes unnecessary security risks. Under this plan, each employee is assigned a metal key that unlocks doors that are also controlled by ACCESS card readers. By replacing the metal keys assigned to each TTC employee with a backup power supply to support ACCESS in the event of a power failure, NRC can reduce the chance that keys will be lost and used to gain unauthorized access to TTC facilities. In addition, reliance on the card readers will allow a more accurate record of access within TTC facilities.

RECOMMENDATIONS

This report makes 17 recommendations to better ensure that ACCESS meets its operational requirements. A consolidated list of recommendations appears on pages 28-29 of this report.

AGENCY COMMENTS

At an exit conference held December 19, 2006, agency managers agreed with the audit findings and recommendations and provided comments concerning the report. We modified the report as we determined appropriate. NRC opted not to submit formal written comments to this final version of the report.

[1] Certification is the comprehensive evaluation of a system's security features and other safeguards that establishes the extent to which a particular design and implementation meet a specified set of security requirements. Accreditation grants the system sponsor the authority to operate the system based on the certification process and other considerations.

[Page intentionally left blank.]

ABBREVIATIONS AND ACRONYMS

ACCESS	ACCESS/PICS
ACCESS/PICS	Access Control and Computer Enhanced Security System/Photo Identification Computer System
C&A	certification and accreditation
DFS	Division of Facilities and Security
FY	fiscal year
NRC	Nuclear Regulatory Commission
HSPD-12	Homeland Security Presidential Directive – 12
IATO	interim authority to operate
ID	identifier
ISSO	information system security officer
IT	information technology
MD	Management Directive and Handbook
OIS	Office of Information Services
TTC	Technical Training Center

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

NRC's automated badging and card reader system is an important component of the agency's physical security program. NRC uses the system to manufacture photo-identification badges for employees, contractors, and visitors and control their access within NRC's headquarters, regional offices, and the TTC. NRC refers to its system as ACCESS/PICS. In this report, the system will be referred to simply as ACCESS, and NRC regional offices and TTC will collectively be referred to as field offices.

Controlling Access

NRC seeks to ensure that only authorized individuals have the freedom to travel unescorted within agency facilities. Individuals may be approved for unescorted access within NRC facilities following the successful adjudication of a background investigation. Approved individuals are issued NRC badges that are programmed to permit unescorted access within NRC facilities. NRC's Division of Facilities and Security (DFS), within the Office of Administration, manages NRC's background investigation and badging process.

Unescorted access may be limited by time of day and location within the facility. For example, NRC employees are automatically allowed 24-hour access, while contractors are typically given access only during business hours. Furthermore, while most staff are afforded access only to NRC's general access areas, some are additionally permitted entry to special access areas based on their specific needs. Special access areas are sections of NRC headquarters space – such as the headquarters day care center, the guard office, or Incident Response Operations – that have restricted access for prior approved individuals only.

NRC also issues temporary badges to employees and visitors. Temporary badges assigned to employees are programmed to allow unescorted access within NRC facilities. The majority of temporary visitor badges are not programmed to allow passage beyond card readers because most visitors must be escorted by an NRC employee or other authorized individual while at NRC premises.

System Description

To gain access inside NRC facilities, individuals place their badges against card readers that are positioned at various locations throughout the buildings. Wiring connects the card readers to a host computer, which stores the access rights afforded to each badge holder and communicates back to the card reader whether access is allowed at a particular door. If access is permitted, the reader displays a green light and the door associated with the reader may be opened. If access is not permitted, the light turns red and the door remains locked. Headquarters has 181 readers; the field offices have between 7 and 28 card readers each.

NRC headquarters card reader

Headquarters uses a different version of ACCESS than the field offices; only the headquarters system manufactures badges whereas all of the systems are used for access control. NRC security guards at headquarters manufacture all headquarters and field offices badges and program them for access to headquarters. Field office badges are then sent to their respective locations where they are programmed to allow access to the employee or contractor's duty station.

The ACCESS systems in headquarters and the field offices do not communicate with each other, and none are connected to a network.

System Data

The headquarters ACCESS system contains 6,409 records of badges (includes employee, contractor, temporary, visitor, and other badges) currently in use at NRC. Records for badges assigned to individuals include social security numbers that are needed for the badge manufacturing process. Field office systems do not store social security numbers. Figure 1 depicts a breakdown of NRC's 6,409 badges by type. Table 1 provides a comparison of the headquarters and field office systems.

Figure 1. NRC Badge Inventory, by Badge Type (N=6,409)

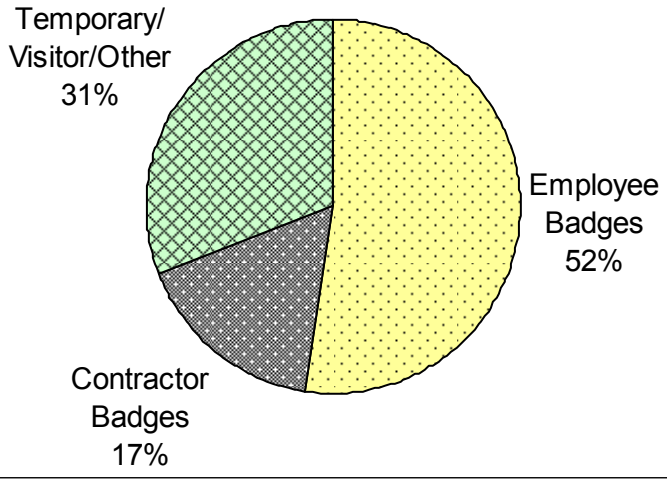

Table 1. Comparison of Headquarters and Field Office Systems

System Characteristic	Headquarters	Field Offices
Manufactures badges	Yes	No
Stores social security number	Yes	No
Controls access	Yes	Yes
Connected to a network	No	No
Badges allow headquarters access	Yes	Yes
Badges allow access to field office[2]	No	Yes

NRC has categorized ACCESS as a "listed" system for information security purposes. The term listed system refers to a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to NRC office or regional operations.

Future Plans

The approximately 15-year old ACCESS system is a legacy system, and NRC plans to replace it in FY 2009 (at the earliest) to comply with HSPD-12. This directive, issued in August 2004,

[2] Regional access control systems can be programmed to recognize headquarters badges.

ordered the establishment of a mandatory Governmentwide standard for secure and reliable forms of identification to be issued by the Government to its contractors and employees. One of HSPD-12's goals is that these identification badges be used for physical access to all Government facilities.

II. PURPOSE

The objective of this audit was to determine whether the current badge access system meets its required operational capabilities and provides for the security, availability, and integrity of the system data. Appendix A contains information on the audit scope and methodology.

III. FINDINGS

NRC's badge access system is capable of providing effective support for NRC's physical security program. However, specific cost-effective actions are needed to enhance this legacy system's usage at NRC until a replacement system is implemented. Auditors identified the following shortcomings with regard to ACCESS and related badge accountability processes:

(A) Weaknesses exist concerning system user access.
(B) The system contains inaccurate data.
(C) Badge accountability measures are inadequate.
(D) System documentation is incomplete or missing.
(E) TTC lacks a backup power supply for ACCESS.

These problems exist because concerns about ACCESS are overshadowed by the agency's plan to replace the system as part of its HSPD-12 solution. Left unaddressed, however, these weaknesses undermine the effectiveness of NRC's physical security approach to control access into and within NRC facilities.

A. Weakness Exist Concerning System User Access

ACCESS does not fully employ the user access controls identified in Management Directive and Handbook (MD) 12.5, "NRC Automated Information Security Program." Specifically, in headquarters and a field office, several people share one user ID,[3] 2 of 11 headquarters users have inappropriate access to the system, and a majority of the headquarters users have been granted the highest level of system access. Noncompliance with MD 12.5 has occurred because there is no routine review of the user access, limitations exist with one site's version of ACCESS, and DFS staff cannot easily define or differentiate the difference among ACCESS user roles. Without adequate user access controls, security information is vulnerable to errors or misuse.

System Requirements

MD 12.5 details the requirements and responsibilities for protection of information and information systems. Specifically, MD 12.5 Appendix A, "NRC Systems Development and Maintenance Security Controls," provides guidance for information system

[3] A user ID is a unique symbol or character string that an individual uses to log on to an information system.

owners. Two security areas that must be addressed when implementing or upgrading an information system are (1) identification and authentication and (2) discretionary access.

Identification and authentication controls provide the capability to establish, maintain, and protect a unique ID and password for each authorized user. MD 12.5 Appendix A states that user IDs must be issued on a one-to-one basis, meaning each system user must have his or her own unique ID.

Discretionary access controls allow the administrator to configure the system to ensure that authenticated users can access and perform operations on only the system resources for which they have authorization. MD 12.5 Appendix A states that access control lists should be used to designate which users have specific permissions. A related concept is the principle of least privilege, which MD 12.5 defines as the practice of restricting user access to data files and levels of access (e.g., read, write, delete) to the minimum amount necessary for job performance.

Inappropriate System Access

ACCESS does not fully employ the user access controls identified in MD 12.5 Appendix A. Specifically, in headquarters and a field office, several people share one user ID, 2 of 11 headquarters users have inappropriate access to the system, and a majority of the headquarters users have been granted the highest level of system access.

Auditors identified two situations where more than one person uses ACCESS through the same user ID. In one case, a single user ID is used by seven headquarters security guards, five of whom work at a particular post in the Central Alarm Station. This post is responsible for monitoring physical security and handling headquarters security issues and officers, who cover the post at different times of the day, can use the common ID to perform tasks in ACCESS. A sixth officer who shares the common ID uses ACCESS each week to disable temporary badges that were loaned but not returned. In the other case, which occurred at a field office,[4] two users share a common user ID on that site's version of ACCESS. These individuals share an office and job responsibilities related to ACCESS.

[4] Auditors also found sharing of IDs in another field office, but this issue was addressed in a separate Office of the Inspector General audit on computer security (OIG-06-A-15, dated July 11, 2006).

Auditors interviewed 22 system users in headquarters and at NRC field offices to determine whether (1) they truly need access to the system and (2) their assigned system role was appropriate. A system role is assigned to each user's login ID and illustrates what level of system rights (read, write, delete) that individual should have.

Most users were appropriately given access to the system. However, 2 out of 11 individuals on the headquarters user list should not have access to the system. One individual, who formerly required system access as part of a prior job assignment, no longer required such access because of a promotion that occurred about 2 years ago. The other individual given access inappropriately was a DFS contractor who performed overall ACCESS system maintenance on a routine basis but was not approved by NRC for any access to work with information technology (IT) systems. NRC requires contractors to undergo a specific type of background investigation before they can work with agency IT systems, and in this case the contractor had not undergone the necessary review.

More than half of the individuals in headquarters with system access had system administrator rights. Of the 11 user accounts assigned to specific individuals to gain access to the headquarters system, 6 had the system administrator role. This level of access allows the users to read and write all the fields, and delete records. Furthermore, an additional two accounts with system administrator rights were not assigned to people, but instead were reserved for the performance of specific tasks. These accounts seem unnecessary, given that the individuals who perform these tasks have their own system administrator accounts associated with their names.

No Routine Review

Access controls for ACCESS are not in compliance with MD 12.5 because there is no routine review of user access. DFS managers did not identify a need to create separate user accounts for security guards stationed at a particular post, and the system version in the field office where the user ID is shared does not allow separate IDs to be created for multiple users with the same role. In addition, DFS staff cannot easily define or differentiate among ACCESS user roles.

Inappropriate individuals have access to the system because DFS staff do not routinely review the user list to determine whether users continue to need system access. In addition, without knowledge of the different levels of access, there is no way to verify that all of the users have the appropriate level or if their access levels need to be adjusted.

DFS allows multiple headquarters security guards to share one user ID because managers did not identify a need to create separate accounts. Furthermore, a software limitation exists within the field office using shared IDs that does not allow multiple users to be granted the same level of access. The system administrator in that field office decided to accept the risk of allowing two people to share one account rather than allow one person to have more access than their counterpart.

DFS assigns the system administrator role to most users because staff who make such assignments cannot readily define the different ACCESS roles but know that the system administrator role will allow users to perform any task needed. A DFS employee stated that identifying the limitations of the different roles has not been a priority for the office.

System Data At Risk

Allowing individuals too much or shared access to system data places the information in the system at risk of inadvertent or deliberate manipulation or misuse. While a DFS manager stated that there have been no known breaches in security, without the proper access controls the system data and NRC security remains vulnerable.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Perform an annual assessment of the user list for ACCESS and modify it appropriately in accordance with least privilege guidance.

2. Require separate user IDs for each user.

3. Assess the cost-effectiveness of updating the field office's version of software to allow multiple user IDs with the same role, and install the updated version if assessment indicates benefits exceed costs.

4. Define and document user roles and associated rights.

B. System Contains Inaccurate Data

ACCESS contains inaccurate data pertaining to special access areas and the current employee population. These data inaccuracies exist because DFS does not impose effective quality assurance measures over access lists or system data. Without accurate information, there is the possibility of security breaches and ineffective control over special access areas.

Data Requirements

Government managers must implement effective management controls over their programs. Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control," states that effective internal control provides reasonable assurance that effective and efficient operations are being achieved. Management Directive 4.4, "Management Controls," states that management controls should reasonably ensure programs achieve their intended results and that reliable and timely information is obtained, maintained, reported, and used for decisionmaking.

ACCESS is designed to provide information on who has access to NRC facilities and the level of access that these individuals have. ACCESS information should accurately reflect the current employee and contractor population and their access rights.

Data Inaccuracies

ACCESS contains inaccurate data pertaining to (1) special access areas and (2) the current employee population. Specifically, people have inappropriate access to special access areas, former NRC employees remain in the system, and some field office location designations are inappropriate.

Special Access Areas

OIG reviewed access lists[5] for five special access areas in headquarters and found that all but one mistakenly included individuals who should not have access to those areas. One list, which allowed 52 people access, included 9 individuals who no longer needed access to this space. The day care center list included 170 names[6] of individuals who no longer needed access,

[5] The lists were generated from ACCESS and show which individuals' badges are programmed to allow access into these special access areas.
[6] Some names were listed more than once.

including one employee who had not had children in the center for more than 4 years. A point-of-contact[7] for a different special access area said the access list for the space had too many people on it because people failed to provide notification when they no longer needed access. This individual was working with DFS to remove those with inappropriate access.

In addition, auditors learned that DFS has given nearly unrestricted access rights to a "super user" group of 28 individuals who are responsible for responding to headquarters security and facility emergencies and therefore need access to NRC's special access areas. These "super users" – primarily staff in DFS – have access to almost every special access area (there is one exception) within NRC headquarters, and while several points-of-contact were generally aware of the "super user" group, they did not know how many individuals or who specifically had such access. One point-of-contact was unaware of the group entirely.

Auditors reviewed the list of "super users," and determined it contained two inappropriate people: a former Executive Director for Operations and a DFS contractor responsible for maintaining the ACCESS system.

Current Employee Population

ACCESS contains former employees and incorrect location designations for some employees. OIG reviewed ACCESS data to determine whether (1) employees who had left NRC during a 3-month period had been removed from the headquarters system at the end of the 3 months (2) employees who had transferred between NRC locations during this period were accurately reflected in the data, and (3) data corrections provided by one field office to headquarters were incorporated into the headquarters system. This review found that 26 of 94 employees who terminated during the 3-month time period still had active records within ACCESS.[8] In addition, three of the eight people who had transferred offices during this timeframe were recorded incorrectly within ACCESS in that the current duty station was incorrect and a new badge had not been issued to the employee that reflected the new duty station.

[7] DFS keeps a list of points-of-contact associated with each special access area. The point-of-contact is the individual designated to communicate with DFS about changes to the special access lists.

[8] Of the 26 individuals who terminated but had not been removed from the headquarters ACCESS system, 17 were field office employees.

With regard to corrections provided by field offices, 7 of 23 corrections requested by a field office had not been incorporated into ACCESS. Table 2 summarizes the results of this data analysis.

Table 2. Data Accuracy Assessment Results

Category	Number of Files Checked	Number With Errors	Error Rate
Terminations	94	26	28 %
Geographical transfers	8	3	38 %
Field office correction requests	23	7	30 %
Total	125	36	29 %

Auditors also determined that two field office systems contain names of many former NRC employees. These field offices add headquarters employees to their systems when they come to the site for a visit/training but do not routinely remove these individuals when the visit/training concludes. In contrast, one field office described a routine, deliberate effort to remove such individuals after they terminate their NRC employment.

Quality Assurance Measures Are Missing

ACCESS data inaccuracies exist because DFS does not impose effective quality assurance measures over access lists or system data. There is no routine review of special access area lists, no oversight to ensure that terminated employees are removed from the headquarters system in a timely manner, and no written guidance to ensure that transfers are reflected accurately in the system or that field offices remove former employees from their systems.

Special Access Areas

There are inappropriate people on the special access area lists because there are no quality control steps to ensure that people are removed from these lists. DFS staff rely on special access area points-of-contact to keep their lists current; however, points-of-contact have differing understandings of this responsibility.

OIG interviewed six points-of-contacts for special access areas, half of whom did not know they could request a list of people with access to the special access areas. One point-of-contact was unaware of the responsibilities of being a point-of-contact. Another point-of-contact performs quarterly checks to ensure their list is accurate, but must proactively request their list from DFS, which does not provide the lists unless asked.

In addition, DFS does not conduct effective reviews of its own super user group**.** While a DFS employee stated that the list is reviewed occasionally during the year, the fact that it contained two individuals who should not be on it suggests the review is ineffective.

Current Employee Population

The headquarters ACCESS system does not accurately reflect the current employee population because (1) DFS staff do not always remove employees from ACCESS in a timely manner and (2) there are no standard operating procedures to ensure that the correct steps are taken in denoting regional transfers within ACCESS. The field office ACCESS systems contain names of employees who no longer work for the agency because there is no guidance instructing these offices to remove former employee names.

Risk of Security Breaches

Without accurate information, there is the possibility of security breaches and ineffective control over special access areas. By allowing people to have inappropriate access to special access areas, there is no guarantee that only the correct people have access to protected space. Having unnecessary names in the system also means the database does not reflect the current population, which could create confusion for DFS employees or security guards who generate temporary badges for employees. Having accurate data will be essential if any of this information will be used in the new HSPD-12 system or if both systems will be maintained concurrently for any length of time.

Recommendations

OIG recommends that the Executive Director for Operations:

5. Institute quarterly quality assurance reviews of system data to ensure that system data is accurate with regard to special access areas, terminated employees, and terminated contractors.

6. Conduct quarterly reviews of super user lists, modify appropriately, and send to special access points-of-contact.

7. Provide official agency list of departures to all field office badging officials to facilitate removal of terminated employees.

8. Write and implement badge access system operating procedures that provides system user guidance and incorporates the preceding three recommendations.

C. Badge Accountability Measures Are Inadequate

NRC lacks adequate control over temporary badges issued to staff and visitors, and over badges issued to contractors. Specifically,

- Temporary badges loaned to staff who forget or lose their badge are not always returned the day they were issued.
- Temporary visitor badges are not inventoried and accounted for on a daily basis at headquarters and three field office sites.
- Contractor badges are not always retrieved promptly or deactivated once it is determined a particular contractor is no longer working for NRC.

Temporary and contractor badges are not always returned promptly because the agency has not asserted measures to enforce these requirements. Daily reconciliation of visitor badges is not performed at headquarters or several NRC field offices because NRC has not enforced this requirement. These weaknesses increase NRC's risk that temporary and contractor badges will be misused to gain unauthorized access into NRC facilities.

Badge Requirements

NRC requirements pertaining to the control of employee, contractor, and visitor badges are included in Management Directive and Handbook (MD) 12.1, "NRC Facility Security Program," and MD 12.3, "NRC Personnel Security Program." These MDs require that:

(1) Temporary badges assigned to employees and contractors be returned at the end of the work day to the guard or receptionist desk from which they were issued.[9]

(2) Temporary badges issued to visitors be inventoried and accounted for on a daily basis.

(3) NRC offices that sponsor a contractor arrange for the immediate return of badges and immediate written notification to DFS when the contractor no longer needs access to NRC facilities.

[9] MD 12.1 states that temporary badges for employees must be returned on a daily basis but does not specifically mention contractor temporary badges. However, a DFS official stated that the expectation is that all temporary badges issued are to be returned daily.

Badge Controls Not Imposed

NRC headquarters and three field offices do not impose daily control requirements over temporary badges assigned to employees, contractors, and visitors. Furthermore, contractor badges are not always returned to NRC and DFS is not always notified promptly when a contractor no longer needs access to NRC facilities.

Temporary Employee and Contractor Badges

NRC headquarters and three field offices do not assess whether temporary employee and contractor badges are returned daily and therefore could not provide definitive numbers concerning staff's failure to return badges. However, based on interviews with staff responsible for tracking temporary badges at headquarters and all five field office sites, auditors learned that it is not infrequent for these badges, which allow unescorted access within NRC facilities, to be retained for more than a day.

According to a headquarters security officer who performs weekly inventories of the temporary badges, on average, seven or eight temporary headquarters badges are not returned each week. Another headquarters security officer recalled that one employee recently returned four temporary badges that had been assigned to this individual concurrently. At the field offices, individuals responsible for tracking temporary badges described occasions where they needed to contact individuals to return temporary badges. In one region, it was reported that about two temporary badges are lost per year while on loan to individuals and therefore never returned.

At headquarters and each of the five field offices, staff who are responsible for tracking temporary badges said that they attempt to retrieve badges after determining the badges were not returned. The number of days it takes to initiate such contact was dependent on the frequency with which the staff reconcile the temporary badges. At two locations, such reconciliation occurred daily; thus retrieval efforts were timely. Retrieval efforts were less timely at the remaining four locations where reconciliations occurred either every few days or weekly.

At headquarters and two field offices, staff stated that they deactivate temporary badges if they are not returned after such retrieval efforts. Again, however, time to deactivate is dependent on how quickly the site becomes aware it is missing.

Temporary Visitor Badges

At headquarters and three field offices, temporary visitor badges are not inventoried and accounted for on a daily basis. Headquarters performs this type of inventory on a weekly basis, but does not follow up when these badges, which are not programmed to permit passage beyond a card reader, are not returned.

At two field offices, visitor badges are tracked on a daily basis. At one site, an expiring paper badge system is used for visitors requiring escorted access.[10] At a different field site, a staff member inventories the visitor badges daily and follows up with the NRC employee escort when a visitor badge is not returned.

Contractor Badges

NRC project officers are not always able to retrieve contractor badges from contractors no longer working on an NRC contract and they do not always notify DFS immediately when a contractor stops working on the NRC contract.

OIG contacted 11 NRC project officers[11] who had experience with contractor badge retrieval and 7 described instances where they had difficulty or were unable to retrieve a contractor's badge. Project officers would usually attempt to retrieve the badge themselves – sometimes for at least a week or two – and when they realized they were not going to be successful, they would usually notify DFS to terminate the contractor's access. One individual never notified DFS that the badge had not been returned and another provided such notification in response to a letter DFS sent to all project officers inquiring about the status of their contractors.

Return Requirements Not Enforced

Temporary badges are not always returned promptly because the agency has not asserted measures to enforce the daily return requirement. For example, there is no requirement for security staff to account for these badges on a daily basis; therefore, a non-returned badge can easily remain undetected. Furthermore, the temporary badges are not deactivated promptly, which allows the

[10] These badges, which are assigned to individuals upon their arrival, gradually change in appearance throughout the day. At time of assignment to a visitor, they feature the visitor's name in black print on a white background. After approximately 8 hours, however, diagonal pink stripes appear clearly on the background, indicating that the person is no longer authorized as a visitor.
[11] One individual was not a project officer, but a contract technical monitor who served as the contact person to deal with DFS on badging matters.

individual to whom such a badge was loaned to keep using it successfully to pass through card reader control points within the NRC facility from which it was assigned.

Daily reconciliation of visitor badges is not performed at several NRC locations because the agency has not enforced this requirement. Furthermore, NRC staff do not make a concerted effort to retrieve these badges because they perceive no risk associated with these badges, which are not programmed to allow the holder beyond any card reader control points.

Contractor badges are not always returned promptly because there is no contractual incentive for the contractor to return the badge. DFS is not always notified promptly about a contractor no longer requiring access because project officers typically try to retrieve the badge before notifying DFS, and in cases where the badge is not retrieved promptly, this notification is subsequently delayed.

Potential for Misuse

All NRC badges could be misused by individuals with malicious intent who are not authorized for entry into NRC facilities. Such individuals could use the badges to gain entry into NRC and then move around freely within the facility to commit petty theft, cause physical harm, or gain access to classified information.

While it is easier to envision the potential harm caused by a lost temporary or contractor badge (which allow unescorted access), a lost visitor badge could also be misused. Visitor badges look similar to non-visitor badges, and someone in possession of one could easily tailgate through a control point behind a non-visitor. NRC needs to tighten its badge control processes to minimize its risk of a non-authorized individual gaining access beyond NRC control points.

Recommendations

OIG recommends that the Executive Director for Operations:

9. Conduct daily reconciliations of temporary badges and disable access for badges not returned.

10. Replace the current visitor badges with expiring paper badges.

11. Include clauses in new contracts imposing a financial penalty for badges not returned.

12. Reiterate to NRC project officers the need to notify DFS immediately when a contractor no longer needs access to NRC facilities.

D. System Documentation Is Incomplete or Missing

NRC has not adhered to agency listed system security requirements for ACCESS or followed up on penetration testing results. This is because the Office of Information Services (OIS) and DFS do not view fulfillment of these requirements as a priority given that (1) ACCESS is a legacy system unlikely to attain certification and accreditation and (2) a Government-wide interoperable solution is expected to replace ACCESS in FY 2009. Without following security requirements, NRC has limited assurance that ACCESS is adequately protected against unauthorized access or other misuse. In addition, ACCESS system owners and users are unable to locate relevant information when needed.

IT Security Requirements

NRC guidance requires the implementation of administrative, technical, and physical security measures appropriate for the protection of NRC information and information systems. Furthermore, it is prudent for agency managers to follow up on reports that identify IT system weaknesses.

Listed System Requirements

According to MD 12.5, listed systems such as ACCESS must have the following:

Inclusion in the OIS master system inventory. This is an overall listing of all NRC information technology systems.

System security plan. This plan addresses the system's functionality, production environment, and security controls and countermeasures to prevent or detect a security incident or mitigate the impact of a security breach. This plan should also include procedures for training individuals permitted system access, procedures for monitoring the effectiveness of security controls, and provisions for continuity of operations in the event of system disruption or failure.

Information system security officer (ISSO). The ISSO is a trusted position with special access to and authority for a system. Responsibilities include developing and monitoring the system's security rules of behavior and other security controls, ensuring that the certification and accreditation process is completed, ensuring that system security program reviews and periodic security testing are completed, and ensuring that the status of remediation activities are tracked and reported until completion.

Certification and accreditation (C&A). This process is defined in footnote 1. The C&A process for listed systems is also fulfilled when the OIS authorizing official issues an interim authority to operate (IATO).[12]

Addressing Identified Weaknesses

Management followup to address report findings and recommendations is a prudent management best practice. Following up on security related reports helps managers identify risks and subsequently determine the acceptable level of risk to ensure that adequate security is maintained.

NRC Has Not Met Requirements

NRC has not (1) adhered to agency listed system security requirements for ACCESS or (2) followed up on penetration testing results.

Listed System Requirements Not Fulfilled

ACCESS appears on the agency's master systems inventory but does not adhere to the other listed system requirements specified in MD 12.5. ACCESS lacks the following:

- System Security Plan
- Information System Security Officer
- Certification and Accreditation

[12] An IATO is issued if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, assets, or individuals is not fully acceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation. The duration established for an IATO should be commensurate with the risk to agency operations, agency assets, or individuals associated with the operation of the information system. When the security-related deficiencies have been adequately addressed, the IATO should be lifted and the information system authorized to operate.

System Security Plan

Despite MD 12.5 requirements, OIS has not approved and DFS has not written a current system security plan. A DFS employee provided auditors with an inadequate and outdated ACCESS security plan that contains the following discrepancies:

- Lacks key information such as the date, approval, and author.
- Incorrectly categorizes ACCESS as a major application.
- Does not base its information sensitivity categorization on current criteria.
- Does not address the controls in place that pertain to the ACCESS stand-alone components that are located in the NRC field offices.

DFS staff were unable to provide clarifying information regarding this security plan, other than acknowledging that it was obsolete. One DFS employee recalled drafting this version of the security plan a long time ago and providing it to an OIS[13] employee for review. OIS provided feedback, which was incorporated by DFS and returned to OIS. However, at that point, the employee recalled, correspondence ended and OIS never provided further feedback.

Information System Security Officer

NRC has not appointed an ISSO for ACCESS as required by MD 12.5. Although several staff are involved with responsibilities concerning the management and operation of ACCESS, the system roles have not been clearly defined. Several individuals conveyed that they have key roles and responsibilities that are similar to those of an ISSO. For example, one DFS employee claimed to be the system point-of-contact, while an employee in the Office of Administration claimed responsibility for handling office IT issues and performing troubleshooting activities related to ACCESS. This employee also claimed to share the ISSO role with another Office of Administration employee; however, there was no indication that this was an official assignment.

Periodic Certification and Accreditation

ACCESS has not been certified and accredited in accordance with MD 12.5. Although an agency official document states that in FY 2005, ACCESS had an interim authority to operate, the agency could not provide any documentation supporting this status. OIS and DFS employees were unable to provide the ACCESS interim

[13] OIS was formerly named the Office of the Chief Information Officer.

authority to operate memorandum or any documentation that would have been reviewed in order to grant the interim authority to operate.

No Follow Up on Penetration Testing Results

OIS conducted a penetration test on ACCESS in the fall of 2005 and provided the results to DFS with the expectation that the weaknesses would be addressed. However, DFS did not address the reported weaknesses and OIS did not follow up to ensure that the weaknesses were addressed.

Requirements Not Given Priority

OIS and DFS managers have not expended resources to complete listed system security requirements for ACCESS or correct the weaknesses identified in the penetration test results because managers do not view these actions as a priority. Management officials representing OIS and DFS have expressed that resources are not being expended on ACCESS given that 1) ACCESS is a legacy system unlikely to attain certification and accreditation and 2) a Government-wide interoperable information technology solution is expected to replace ACCESS within the next 2 to 3 years.

OIG acknowledges that it would not be cost-effective to implement the full scope of security controls for ACCESS; however, certain controls are essential to mitigate risks associated with the system. NRC needs to pursue the cost-effective controls and document why other controls will not be pursued at this time.

Limited Assurance of Protection

Without adhering to NRC system security requirements and following up on penetration testing results, NRC has limited assurance that the system is sufficiently protected against unauthorized access, use, disclosure, disruption, modification, or destruction of information and property. In addition, ACCESS system owners and users are unable to locate relevant information when needed.

Recommendations

OIG recommends that the Executive Director for Operations:

13. In accordance with NRC requirements for listed systems, develop an ACCESS system security plan and appoint an Information System Security Officer.

14. Develop documentation to support the ACCESS interim authority to operate.

15. Complete the actions necessary to address the ACCESS weaknesses contained in the penetration test report.

E. TTC Lacks Backup Power Supply for ACCESS

TTC's card reader contingency plan in the event of a power failure is workable, but causes unnecessary security risks. Under this plan, each employee is assigned a metal key that unlocks doors that are also controlled by ACCESS card readers. By replacing the metal keys assigned to each TTC employee with a backup power supply to support ACCESS in the event of a power failure, NRC can reduce the chance that keys will be lost and used to gain unauthorized access to TTC facilities. In addition, reliance on the card readers will allow a more accurate record of access within TTC facilities.

Backup Power Benefit

It is important from a security perspective to have an ACCESS contingency plan in place to use if electricity fails. Contingency plan elements can include coverage at control points by security guards, an uninterrupted power supply that would allow continued coverage by ACCESS during a power outage, and keys that staff would use if the uninterrupted power supply failed.

TTC Lacks Backup Power

TTC's contingency plan is workable, but causes an unnecessary security risk. To deal with power failures that occur periodically at TTC, the approximately 30 staff are assigned regular metal keys, as well as key cards, and either will work to gain entry into and within TTC facilities. If a metal key is lost, which happened recently, all locks at TTC must be rekeyed. Furthermore, the metal key is a standard key that can easily be copied by a locksmith.

In contrast, two of NRC's regional offices that have uninterruptable power supplies also assign metal keys to certain staff to be used if there is a complete power failure. In one region, the keys will not work unless there is such a failure. In the other region, usage of the keys in the absence of a complete power failure triggers an alarm.

Keys Used Instead

Staff are given metal keys as a backup to use in the event of power failure at TTC because the facility lacks an uninterrupted backup power supply that would activate during a power outage.

Security Is Weakened

By relying on standard metal keys as a backup to TTC's badge reader system, the agency risks that keys will be lost or duplicated and used to gain unauthorized access to TTC facilities. Furthermore, because employees always have the option to override ACCESS by using a key for entry, the agency lacks an accurate record of access into and within TTC facilities. Replacing the metal keys with an uninterruptible power supply backup will enhance security at TTC and reduce the burden on staff who perform quarterly inventories of the keys assigned to TTC employees.

Recommendations

OIG recommends that the Executive Director for Operations:

16. Assess the cost effectiveness of providing power backup for the TTC badge access system.

17. Alternatively, limit distribution of keys to a smaller number of TTC staff and use security keys that cannot easily be duplicated.

IV. AGENCY COMMENTS

At an exit conference held December 19, 2006, agency managers agreed with the audit findings and recommendations and provided comments concerning the report. We modified the report as we determined appropriate. NRC opted not to submit formal written comments to this final version of the report.

V. CONSOLIDATED LIST OF RECOMMENDATIONS

1. Perform an annual assessment of the user list for ACCESS and modify it appropriately in accordance with least privilege guidance.

2. Require separate user IDs for each user.

3. Assess the cost-effectiveness of updating the field office's version of software to allow multiple user IDs with the same role, and install the updated version if assessment indicates benefits exceed costs.

4. Define and document user roles and associated rights.

5. Institute quarterly quality assurance reviews of system data to ensure that system data is accurate with regard to special access areas, terminated employees, and terminated contractors.

6. Conduct quarterly reviews of super user lists, modify appropriately, and send to special access points-of-contact.

7. Provide official agency list of departures to all field office badging officials to facilitate removal of terminated employees.

8. Write and implement badge access system operating procedures that provides system user guidance and addresses the preceding three recommendations.

9. Conduct daily reconciliations of temporary badges and disable access for badges not returned.

10. Replace the current visitor badges with expiring paper badges.

11. Include clauses in new contracts imposing a financial penalty for badges not returned.

12. Reiterate to NRC project officers the need to notify DFS immediately when a contractor no longer needs access to NRC facilities.

13. In accordance with NRC requirements for listed systems, develop an ACCESS system security plan and appoint an Information System Security Officer.

14. Develop documentation to support the ACCESS interim authority to operate.

15. Complete the actions necessary to address the ACCESS weaknesses contained in the penetration test report.

16. Assess the cost effectiveness of providing power backup for the TTC badge access system.

17. Alternatively, limit distribution of keys to a smaller number of TTC staff and use security keys that cannot easily be duplicated.

[Page intentionally left blank.]

Appendix A

SCOPE AND METHODOLOGY

Auditors evaluated NRC's badging and card reader system to determine whether the system meets its required operational capabilities and provides for the security, availability, and integrity of the system data.

The Office of the Inspector General audit team reviewed relevant criteria, including NRC MD 12.5, "NRC Automated Information Security Program," MD 4.4, "Management Controls," MD 12.1, "NRC Facility Security Program," and MD 12.3, "NRC Personnel Security Program." Other relevant criteria related to the management controls required for the badge access system includes Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control."

Auditors interviewed Office of Administration and OIS staff to learn their roles and responsibilities as they pertain to ACCESS. Auditors also interviewed TTC, regional, and headquarters staff with roles in NRC's badging process to assess their understanding of the process and assess whether their day-to-day activities are conducted in accordance with requirements.

Auditors reviewed the badging process as implemented in headquarters, regional offices, and the TTC to assess whether the NRC's process and procedures met system security objectives. Auditors also reviewed and analyzed system data concerning access rights and entry into special access building areas.

This work was conducted from May 2006 through October 2006, in accordance with generally accepted Government auditing standards and included a review of management controls related to the audit objective. The work was conducted by Beth Serepca, Team Leader; Judy Gordon, Audit Manager; Vicki Foster, Senior Management Analyst; and Rebecca Underhill, Auditor.