AUDIT REPORT

Audit of NRC's Integrated Personnel Security System

OIG-06-A-06 January 9, 2006

January 9, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S INTEGRATED PERSONNEL SECURITY SYSTEM (OIG-06-A-06)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Integrated Personnel Security System* (IPSS).

The audit found that while many IPSS users report that the system is easier to use than its predecessor systems and provides more functionality, IPSS does not perform in accordance with its required operational capabilities. Specifically,

- The system is not fully functional.
- System data is inaccurate and missing.
- System checks to ensure data accuracy and correspondence between related data items are inadequate.
- Security measures are inadequate or missing.
- IPSS lacks a records disposition schedule.

This report makes 17 recommendations to strengthen the Integrated Personnel Security System.

During an exit conference on December 22, 2005, NRC officials provided informal comments concerning the draft audit report. These comments have been incorporated, as appropriate, in our final report.

If you have any questions, please call Beth Serepca at 415-5911 or me at 415-5915.

Attachment: As stated

Electronic Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, 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
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
Luis A. Reyes, Executive Director for Operations
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
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Janet R. Schlueter, Director, Office of State and Tribal Programs
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

EXECUTIVE SUMMARY

BACKGROUND

The Nuclear Regulatory Commission (NRC) Division of Facilities and Security (DFS) administers NRC's facility and personnel security programs. Its responsibilities include making determinations concerning security clearances and access, administering the drug testing program, and physically protecting NRC facilities.

In September 2002, DFS initiated a contract to develop a new integrated computer system to support NRC's personnel and facility security programs. This new Integrated Personnel Security System (IPSS) was expected to replace several DFS information technology systems. Although IPSS was deployed in October 2003 and DFS staff use the system daily to manage the personnel and facility security programs, development is still underway.

PURPOSE

The objective of this audit was to determine if IPSS meets its required operational capabilities.

RESULTS IN BRIEF

Although many IPSS users report that the system is easier to use than its predecessor systems and provides more functionality, IPSS does not perform in accordance with its required operational capabilities. Specifically,

- The system is not fully functional.
- System data is inaccurate and missing.
- System checks to ensure data accuracy and correspondence between related data items are inadequate.
- Security measures are inadequate or missing.
- IPSS lacks a records disposition schedule.

IPSS Is Not Fully Functional

Despite contract requirements for the following system functionalities, IPSS (1) does not provide a complete list of employees and contractors due for clearance or access reinvestigation, (2) does not provide drug testing management capabilities, (3) has not provided reliable report-generating capabilities to enable DFS staff to make quality assurance determinations, and (4) does not allow for the deletion of records.

These problems exist because NRC did not follow the agency standard system development life cycle process, and the system was deployed before development was complete. As a result, DFS staff lack IPSS reports to ensure the effectiveness of the security program, must maintain duplicate systems for drug testing and badge management, cannot delete flawed records from IPSS, and cannot determine with confidence when and at what cost the system will be fully functional.

Data Inaccurate and Missing

Key information within the IPSS system is inaccurate, missing, or incorrectly displayed. Of 262 files analyzed by the Office of the Inspector General (OIG), 119 files contained one or more data errors. These errors occurred because DFS management did not provide users with adequate guidance and have implemented inadequate quality control procedures. Without accurate IPSS data, DFS cannot ensure that reinvestigations are performed in a timely manner, as required.

IPSS Checks Are Inadequate

IPSS lacks required system checks to assure correspondence between (1) badge type and clearance type and (2) clearance type and investigation type. The system also lacks logical date checks to ensure data accuracy. These issues exist because problems with system checks were not identified during user acceptance testing and because too few checks were included in system requirements documents. This lack of checks could result in the disclosure of classified information to those unauthorized for such access; it has already resulted in the issuance of incorrect badges to two NRC employees and in IPSS data errors.

System Security Measures Inadequate or Missing

IPSS does not follow several important security practices outlined in its security plan, including assigning users with the least amount of access needed to perform their job, having the capability to identify when and how the system is used, and having users sign an integrity statement. IPSS security measures are inadequate because DFS managers performed ineffective oversight of system role assignments and were unaware of the risks posed by a lack of audit trails and an integrity statement. As a result of these shortcomings, personnel security information is vulnerable to misuse, both intentional and unintentional.

IPSS Lacks Records Disposition Schedule

IPSS lacks a records disposition schedule because the Office of Information Services (OIS) failed to inform DFS of this need during the system development process. As a result, the system is not in compliance with Federal records retention requirements.

RECOMMENDATIONS

This report makes 17 recommendations to better insure IPSS meets its operational requirements. A consolidated list of recommendations appears on pages 23-24 of this report.

AGENCY COMMENTS

At an exit conference held on December 22, 2005, NRC officials generally agreed with the report's findings and recommendations and provided comments concerning the report. In addition, they stated that they were aware of problems with IPSS prior to receiving the draft report. We modified the report as we determined appropriate. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

ABBREVIATIONS AND ACRONYMS

DFS	Division of Facilities and Security
IPSS	Integrated Personnel Security System
NARA	National Archives and Records Administration
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OIS	Office of Information Services
OPM	Office of Personnel Management

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

DFS administers NRC's facility and personnel security programs. Its responsibilities include:

- Making initial and continuing eligibility determinations concerning security clearances and access, and ensuring that all employees have security clearances in accordance with Atomic Energy Act requirements. [1]

- Administering NRC's drug testing program, which tests designated NRC employees and applicants for the presence of illegal drugs.

- Physically protecting NRC facilities through the use of badge access and other systems.

In September 2002, DFS contracted with PEC Solutions, Inc., to develop a new integrated computer system to support NRC's personnel and facility security programs. This new system, IPSS, was expected to replace the prior personnel security system and five other DFS security systems. One of the goals for IPSS was to integrate relevant security functions performed by these systems, such as badge management, classified visit tracking, personnel security tracking, and drug testing management. The integrated system would allow personnel security information to be entered once and then be available for each of these functions to draw from. (See Appendix B for more information on IPSS.) IPSS was to be Web-enabled and allow users access through the NRC Intranet. The contract anticipated system implementation by June 2003 at a total contract cost of $386,850.

[1] Pursuant to the Atomic Energy Act of 1954, as amended, all NRC employees must have a security clearance; under NRC's system, employees receive either an L clearance, which equates to a Confidential or Secret clearance; a Q clearance, which equates to a Top Secret clearance; or an L(H) designation for employees who hold high public trust positions. In addition, NRC requires contractors to have (1) a security clearance to work with classified information or in a position of high public trust, (2) IT access to work with NRC sensitive IT systems and information, or (3) building access to be permitted continuous unescorted access within headquarters or regional office facilities (but not access to sensitive IT systems or information).

Although IPSS was deployed on October 17, 2003, [2] and DFS staff use the system daily to manage the personnel and facility security programs, work to develop IPSS to meet initial contract requirements continues and the contract is in its seventh modification. Contract obligations thus far total $550,266.57 and DFS officials anticipate that up to $90,000 more will be needed to finish developing the system by a new target date of December 2006.

IPSS has 78 authorized users. See table 1 for a listing of users and their IPSS-related duties.

Table 1

Job Title (# of Staff in Category)	Description of IPSS Duties
Processors (3)	Enter personnel security tracking data (e.g., clearance type, dates of background investigations, personal history information) into IPSS and perform the bulk of IPSS data entry tasks.
Adjudicators (6)	Review IPSS information as part of the clearance/access adjudication process, but rarely enter data.
Security Guards (47)	Assign permanent and temporary badges to employees, contractors, and classified visitors. Assure that assigned badges are appropriate for the person's clearance or access level.
Facility Security Specialists (5)	Run quality assurance reports on access issues.
Other Users (17)	Includes other DFS users, non-DFS staff who support IPSS, and agency managers who have been granted limited access to IPSS information due to their job responsibilities.

For information security purposes, IPSS is classified as a major application. This Office of Management and Budget categorization means the system requires special attention to security due to the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

IPSS contains records on approximately 21,500 individuals (active and inactive employees, contractors, consultants, licensees, and others).

[2] A DFS manager explained that for a period of time preceding this date, DFS was using both IPSS and the predecessor personnel security systems to store personnel security data, but that DFS stopped using one of the major predecessor systems on October 17.

II. PURPOSE

The audit objective was to determine whether IPSS meets its required operational capabilities. Appendix A contains information on the audit scope and methodology.

III. FINDINGS

Although many IPSS users report that the system is easier to use than its predecessor systems and provides more functionality, IPSS does not perform in accordance with its required operational capabilities. Specifically,

A. The system is not fully functional.

B. System data is inaccurate and missing.

C. System checks to ensure data accuracy and correspondence between related data items are inadequate.

D. Security measures are inadequate or missing.

E. IPSS lacks a records disposition schedule.

These problems exist because NRC did not follow the agency standard system development life cycle process and did not employ adequate quality assurance measures over the system and its data. As a result, some important system data is unreliable and the system does not fully support the agency's personnel and facility security programs as originally intended.

Given the extent of problems identified with IPSS and changes in Federal personnel security requirements, the agency needs to pursue all recommendations identified in this audit report, including a summary recommendation to conduct a cost-benefit analysis to determine the value of continuing to develop IPSS versus purchasing an alternative product.

A. IPSS Is Not Fully Functional

Despite contract requirements for the following system functionalities, IPSS:

- Does not provide a complete list of employees and contractors due for clearance or access reinvestigation.
- Does not provide drug testing management capabilities.
- Has not provided reliable report-generating capabilities to enable DFS staff to make quality assurance determinations.
- Does not allow for the deletion of records.

These problems exist because the OIS project manager did not follow the agency standard system development life cycle process, and the system was deployed before development was complete. As a result, DFS staff lack IPSS reports to ensure the effectiveness of the security program, must maintain duplicate systems for drug testing and badge management, cannot delete flawed records from IPSS, and cannot determine with confidence when and at what cost the system will be fully functional.

Required Functionalities

The IPSS contract and the IPSS project plan include specific system functionalities required to support NRC's personnel and facility security programs. These requirements include, among others, a system capability to (1) alert DFS staff of all individuals coming due for background reinvestigations; (2) allow DFS to create and maintain drug testing records for NRC employees, applicants, and selected contractors and to create and maintain a drug testing pool of selected individuals; (3) provide users with direct access to pre-defined reports to help manage the security program; and (4) allow the capability to delete a personnel security record.

Problems With Required Functionalities

Despite these system requirements, none of the four functionalities listed above exist dependably within IPSS.

List of Individuals Due for Reinvestigation

The IPSS Notifications Page, which is the IPSS report DFS uses to determine who needs to be reinvestigated for continued security clearance or access, does not identify all individuals whose data indicate they are due for reinvestigation. Auditors examined the IPSS records for 262 randomly selected employees and contractors and identified that 14 of these individuals had data indicating they were overdue for reinvestigation by up to 7 years. Yet, none of these individuals appeared on the Notifications Page and none had records indicating a request had been submitted by NRC to the Office of Personnel Management[3] to initiate a reinvestigation.

OIG provided this information to DFS staff, who acknowledged that IPSS was not identifying reinvestigations correctly from the database. Subsequently, DFS staff reviewed each of the 14 cases and determined that, in fact, not all of these individuals were overdue for reinvestigation. According to their assessment, one was overdue, four were terminated although this was not noted in IPSS, and the others were not overdue but appeared to be so because their data in IPSS was in error (see finding B for elaboration on IPSS data inaccuracies). A DFS manager stated that staff have since corrected these particular data inaccuracies within IPSS, initiated the reinvestigation process for the overdue individual, and intend to pursue correction of the underlying problem with the Notifications Page.

Drug Testing Management

IPSS' drug testing management functionality is inoperable and remains under development. Although this was one of the basic contract requirements for IPSS, DFS staff explained that the contractor has yet to implement this component. They said the contractor has been working closely with DFS staff to develop the component.

Access to Reports

A portion of IPSS' pre-defined reporting capability has never functioned properly, and even when the reports appear to be working, DFS staff expressed a lack of confidence about their accuracy. According to the contract and to the project plan, IPSS was to feature more than 50 pre-defined queries and reports to

[3] Most background investigations for NRC employees are conducted by the Office of Personnel Management (OPM). The exception is the presidentially appointed Chairman, Commissioners, and Inspector General, whose background investigations are conducted by the Federal Bureau of Investigation.

allow users direct and timely access to information about the security program. IPSS was also supposed to provide an ad-hoc reporting capability to let users design new queries and reports and save them for future use. DFS staff said they need these reports to perform routine quality assurance checks of the security program. For example, the reports help to ensure that temporary badges issued have been returned each day, clearance type matches badge type, and contractors who are not permitted 24-hour access to NRC facilities are not gaining access during non-business hours.

DFS staff said instead of using the IPSS reports, they make requests of the system administrator for the reports they need. They also rely on other systems, which IPSS was supposed to replace, to perform the reporting tasks that IPSS was intended to perform.

Deletion of Records

IPSS does not allow records to be deleted, therefore, flawed records must remain in the system until a request can be made to OIS database management staff to use a "back-door" approach to delete records via the database server. DFS staff said that although the IPSS contract and project plan state the system will allow the deletion capability, a former DFS manager who no longer works for NRC insisted the feature would pose a security risk and consequently the feature was not pursued. OIG contends that omitting this feature is problematic and there are preferable means to prevent misuse.[4]

OIS Provided Insufficient Support

These system problems exist because OIS has not provided essential and required support to DFS during the IPSS development process and because DFS staff deployed the system prematurely.

According to both methodologies NRC has used over the past 4 years to facilitate systems development, OIS is required to support the program offices. According to an OIS manager, the focus of the support has shifted from a more technical approach to more of an overall project management approach, but in either case OIS is required to assist offices throughout the development process. According to the OIS manager, the OIS employee assigned to help

[4] One means would be to allow a single individual who is not a regular system user (such as the system administrator or system security manager) to have this capability, and use audit trails to ensure the feature is used appropriately.

DFS with IPSS did not follow the agency standard system development life cycle process. According to the manager, this employee has since retired from NRC and a replacement was not assigned to assist DFS further.

DFS managers recognized that IPSS was deployed prematurely and that more problems should have been resolved before making the transition from the old systems to the new. At that time a decision was made to utilize a partially completed system as the prior personnel security system was failing and data was corrupt. One manager said the decision to deploy the system in 2003 was made by two managers who no longer work in DFS and who were focused on staying close to the implementation deadline.

Impact on Security Program

Due to the problems with IPSS, the system does not provide the desired assurance that NRC is in compliance with security clearance and access reinvestigation requirements. In addition, DFS cannot provide effective oversight over the security program, the office is forced to maintain security systems that IPSS was intended to replace, and users are confused by incorrect data records. Furthermore, the cost and time required to develop IPSS continues to escalate beyond initial expectations; current predictions anticipate the system will be completed by December 2006.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Assign an Office of Information Systems project manager to work closely with DFS for the remainder of the IPSS development process.

2. Correct the reinvestigations notifications report so that all overdue cases are identified and submitted for reinvestigation.

B. DATA INACCURATE AND MISSING

Key information within the IPSS system is inaccurate, missing, or incorrectly displayed. Of 262 files analyzed by OIG, 119 files contained one or more data errors. These errors occurred because DFS management did not provide users with adequate guidance and have implemented inadequate quality control procedures. Without accurate IPSS data, DFS cannot ensure that reinvestigations are performed in a timely manner, as required.

Required Controls

In accordance with Federal 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. NRC 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.

The NRC reinvestigation program is designed to ensure that NRC employees and contractors receive the necessary background investigations to support their continued eligibility for security clearances and access assignments. Management Directive 12.3, "NRC Personnel Security Program," establishes that DFS will initiate a reinvestigation every 5 years for Q and L(H) (high public trust) clearances and every 10 years for L clearances and IT access. According to a DFS manager, the 5 or 10 year period begins when the most current investigation was closed by OPM, provided that the investigation allowed the issuance or continuation of a security clearance.

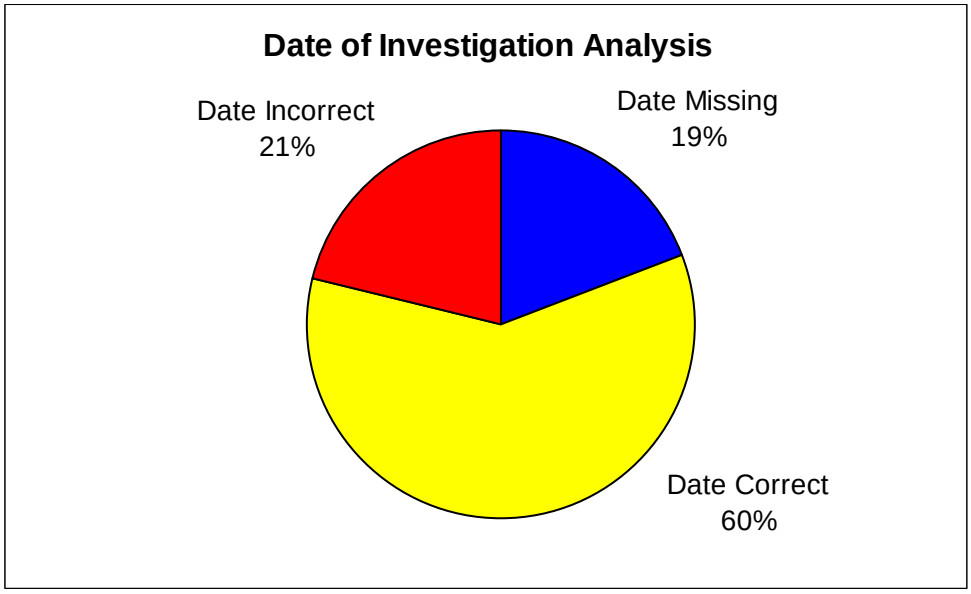
Information Is Inaccurate, Missing, and Incorrectly Displayed

Despite DFS reliance on IPSS, key information within the system is inaccurate, missing, or incorrectly displayed. Specifically,

- Information used to track reinvestigations is inaccurate or missing.
- Other information within IPSS contains errors.
- Data concerning clearance status is incorrectly displayed.

Reinvestigation Data Inaccurate or Missing

While IPSS is a tool for ensuring that reinvestigation requirements are met, key information within the system is inaccurate and/or missing. DFS staff rely on IPSS to track employees and contractors who need reinvestigations. Each day, IPSS generates and updates a Notifications Page that lists individuals coming due for a reinvestigation; this information is pulled by a program which relates to a field within IPSS called "date of investigation." This date of investigation field contains the date the last investigation was closed by OPM. An OIG analysis of this field found that 105 out of 262 files[5] randomly selected for review contained an error in this field. Of the 105 files with errors, 50 files were missing a date in the field. The other 55 files had an error in the date reflected in IPSS. The following figure illustrates this breakdown.



In some cases, the data inaccuracies were due to different choices made by staff on which date to enter. For example, during a short period of time around 1997, reinvestigations were conducted for L clearances without sending paperwork to OPM. This reinvestigation, called a file and fingerprint check, consisted of running checks on fingerprints and searching law enforcement databases for any negative information. The adjudicator would then adjudicate the case based on this information and grant a continued clearance if the outcome was acceptable. When IPSS was implemented, DFS managers determined that for individuals

[5] OIG reviewed 262 personnel security files located within the DFS vault. Auditors randomly pulled active employee and contractor files and compared the information within the paper file to the information within IPSS.

whose last reinvestigation was a file and fingerprint check, the date of investigation within IPSS should reflect the date the adjudicator signed the paperwork. Of the 262 files OIG reviewed, 15 had file and fingerprint checks as the last reinvestigation. Of the 15 file and fingerprint checks, 10 contained errors in the dates. In 7 of these 10 errors DFS staff entered the previous OPM investigation closed date as the date of investigation within IPSS.

At DFS' request, OIG provided DFS with each of the error examples listed above. According to a DFS manager, each example was subsequently reviewed and corrections were made to IPSS and the paper files as appropriate.

Other Data Errors

In addition to errors in the date of investigation, there were other data errors within IPSS. These occurred with social security numbers, names, and clearance type. Of the 262 files OIG reviewed, 5 individuals had 2 IPSS files; one with the correct social security number and one with an error in the number that cannot be deleted from the system (see Finding A for more information on this issue). In addition, 11 files contained errors in either the first or last name, 3 files had errors in both the first and last name, and 5 files contained inconsistencies in the clearance or access level.

Clearance Data Incorrectly Displayed

Data concerning clearance status is incorrectly displayed in IPSS. IPSS uses a split screen to track an individual's clearance history. The left side tracks access (e.g., temporary access, IT access, building access) and the right side tracks clearances (Q, L(H), or L). OIG's review of IPSS data found that in every instance where an employee or contractor has been issued a clearance, information relative to status (e.g., active, terminated, pending) was entered on the access portion of the split screen. Processors explained that this occurs because within IPSS there are mandatory fields that must be entered before the new record will be accepted by the system. Subsequently, information appears on both the access and clearance sides of the screen when it should appear only on the clearance side.

Oversight Is Inadequate

Key information within IPSS contains errors because DFS management did not provide users with adequate guidance and users have created workarounds. In addition, quality control procedures are not adequate.

Inadequate Guidance

Errors within IPSS occurred because DFS lacks written guidance and effective quality control over the system. DFS has not provided users with useful written guidance. Of 22 IPSS users interviewed by OIG, 14 said they never received written guidance. Four individuals interviewed said that when IPSS was first implemented, they received a user guide that the contractor created. This user guide was not updated as changes were made to the system and therefore it is not applicable for how the system is currently used.

In addition, the processors, who are responsible for entering most of the information in IPSS, do not receive formal written notification of policy changes on how to enter information within the system. Instead, a DFS manager meets with the processors to convey changes verbally. Sometimes the DFS manager follows up with an e-mail confirming the guidance.

User Workarounds

Clearance information in IPSS is incorrectly displayed because of a design flaw within IPSS that requires the completion of the access date regardless of whether the record is for someone with a clearance or access. Due to this design flaw, DFS processors have created workarounds (enter clearance information in the access fields as well as the clearance fields) to allow them to enter records in the system.

Inadequate Quality Control Measures

Another reason for IPSS data errors is that DFS' quality control measures are ineffective. DFS currently has a quality control procedure that includes two separate checks of system data. The first check is performed by the processors when an individual submits his or her paperwork to DFS to process for reinvestigation; at this point, the processors are responsible for checking the data within IPSS, including name, date of birth, and last investigation. The adjudicator performs the second check upon receipt of an investigation to adjudicate; they check the same information that the processor reviewed. Given the extent of data problems within IPSS, it is apparent that these measures are ineffective in ensuring the correct information is within the database.

Impact on Clearance Process

Missing and inaccurate data within IPSS can lead to reinvestigations not being performed in a timely manner. If the date of investigation is incorrect, IPSS begins the reinvestigation countdown at the incorrect date. In addition, when there is no date of investigation for an individual within IPSS, the Notifications Page will never identify this individual as coming due for a reinvestigation.

Having inappropriate required fields within IPSS caused additional information to be added to the system. This additional information can be incorrect or misleading to system users. For example, some users appear to be terminated when they have an active clearance because of the required entries in the access section. This could cause confusion for the security guards if the employee needs a temporary badge.

Recommendations

OIG recommends that the Executive Director for Operations:

3. Develop and implement a consolidated data entry guide for IPSS users and update it every 6 months or as needed.

4. Review and correct the most recent reinvestigation dates within IPSS.

5. Change IPSS to eliminate the requirement to duplicate clearance data within the system.

6. Eliminate data that was purposely duplicated as a workaround in IPSS records for individuals with a clearance.

7. Perform top-to-bottom cleanup effort of every active file; support this effort with clear written guidance as to what data goes in what field.

8. Develop and implement an overall quality control approach to ensure continued data accuracy.

C. IPSS CHECKS ARE INADEQUATE

IPSS lacks required system checks to assure correspondence between (1) badge type and clearance type and (2) clearance type and investigation type. The system also lacks logical date checks to ensure data accuracy. These issues exist because problems with system checks were not identified during user acceptance testing and because too few checks were included in system requirements documents. This lack of checks could result in the disclosure of classified information to those unauthorized for such access; it has already resulted in the issuance of incorrect badges to two NRC employees and in IPSS data errors.

Necessary System Checks

Computer systems cannot effectively support business operations unless they include sufficient checks to (1) highlight illogical actions to prevent misapplication of the business operation's rules and (2) ensure that key data they process is accurate and reliable. To this end, the IPSS project plan stated that IPSS would:

- Ensure a correlation is made between clearance/access type and type of badge issued so that no one could be assigned a badge that was inappropriate to their clearance or access.

- Make appropriate notification if the investigation on record is insufficient for the clearance requested or issued.

System Checks Are Missing

IPSS is missing fundamental system checks to facilitate the correct application of DFS policies and to ensure data accuracy. Auditors tested both the production and test versions[6] of IPSS for these checks and balances and found that neither version:

- Prevented the assignment of an inappropriate badge type.

- Ensured a correlation between investigation and clearance type.

- Prevented the entry of illogical dates.

[6] The production version of IPSS is the version that DFS is now using to support its daily operations. The test version is the version the contractor has improved, based on required enhancements, but which has not been implemented for use on a daily basis.

Specifically, system tests conducted by OIG allowed the authorization of a Q-clearance badge to employees without Q-clearance status, allowed the authorization of an L-clearance badge to employees without L-clearance status, and allowed the authorization of clearances and badges to employees when there was no corresponding investigation information entered in the system.[7]

Furthermore, an analysis of 262 IPSS records revealed at least 8 examples of illogical date entries that, if flagged to users, could have prompted correction of the dates, in turn, which would increase the accuracy of IPSS data. These were cases where the predictable chronological sequence of (a) sending a request for investigation to OPM, (b) OPM's closure date for the investigation (which, as noted previously, NRC uses to begin the countdown to the next reinvestigation), and (c) the date NRC receives the case back from OPM was obviously not reflected by the dates in IPSS. In these cases, the date that NRC received the closed case from OPM preceded the date the case was closed.

User Testing Was Inadequate

IPSS does not include basic system checks to prevent issuance of wrong badges or assignment of inappropriate clearances because user acceptance testing was inadequate to uncover the problems. Date logic checks were not included in the IPSS contract or project plan and consequently the contractor was not required to build them into the system.

According to DFS staff who were involved in testing IPSS prior to acceptance, they were not provided with formal instructions on how to test the system and they did not apply a methodical approach to see whether project plan requirements were included in the final system. DFS staff said they tested the system by taking actions they thought they would take as system users. A DFS manager provided us with one PEC document, dated April 2004 (6 months after DFS deployed IPSS), which contained general testing suggestions but was not intended to test the full capabilities and functions of IPSS.

DFS managers could not explain why date checks were not included in the system; one manager recalled discussions that such checks would be included, but did not know why they were not issued as system requirements.

[7] OIG conducted tests of the built-in system controls. Although the system allowed auditors to authorize inappropriate badge assignments, none were actually issued as a result of the test.

Risks Posed By Missing Checks

Because IPSS lacks system checks to ensure that badges issued correspond to clearance type and that clearance type corresponds to investigation type, it is possible that an employee or contractor will be given inappropriate access to classified information. Furthermore, two regional employees who had not received their security clearances were mistakenly issued badges indicating they had L clearances. These occurrences were identified by the region's security officer and resolved before either individual came into contact with classified information. Finally, system checks would have prevented errors in OPM investigative case closing dates in cases where the case closed date entered in IPSS preceded the entry for the date the case was sent to OPM.

Recommendations

OIG recommends that the Executive Director for Operations:

9. Fix the planned controls to prevent incorrect badge issuance and incorrect clearance assignment.

10. Add date logic controls to ensure that OPM investigation dates follow in logical chronological order.

D. SYSTEM SECURITY MEASURES INADEQUATE OR MISSING

IPSS does not follow several important security practices outlined in its security plan, including assigning users with the least amount of access needed to perform their job, having the capability to identify when and how the system is used, and having users sign an integrity statement. IPSS security measures are inadequate because DFS managers performed ineffective oversight of system role assignments and were unaware of the risks posed by a lack of audit trails and an integrity statement. As a result of these shortcomings, personnel security information is vulnerable to misuse, both intentional and unintentional.

System Security Requirements

The IPSS security plan[8] acknowledges that individuals authorized to have access to information systems potentially impose the greatest harm to those systems, both accidentally and intentionally. The IPSS security plan lists various security controls to prevent and detect harm to the system. These controls include least privilege and audit trails. Least privilege is the practice of restricting a user's access to data files and the levels of access (e.g., viewable and editable) to the minimum amount necessary to perform his or her job. According to the security plan, audit trails are used to monitor IPSS user activity. Audit trails are a record showing who has accessed the system and what operations he or she has performed during a given period of time. The security plan states that these mechanisms need to be implemented in order to improve the security of the system and the system data.

In addition, the system security plan contains an integrity statement that provides guidelines for users on when and how to use IPSS. The security plan suggests that each user should sign this document to ensure that they know and understand their responsibilities.

Several Security Practices Are Not Followed

IPSS does not follow several important security practices outlined in its security plan. Specifically,

[8] The Computer Security Act requires all Federal agencies to develop and implement a plan for the security and privacy of computer systems that contain sensitive information. In addition, the Act requires Federal agencies to review and update these plans every 3 years.

- Least privilege is not followed in that some users are allowed too much access to the data, and other users have been inappropriately assigned the wrong access type.

- IPSS does not contain audit trails.

- Users do not sign an integrity statement on appropriate use of the system.

Least Privilege Not Followed

The least privilege principle was not followed for IPSS in that some roles allow too much access and others have been inappropriately assigned.

IPSS allows users to have different levels of access to the system based on the user being assigned one or multiple roles. These roles determine what screens the user can view and, within a screen, what fields are viewable and/or editable. As of June 24, 2005, IPSS had 12 roles that could be assigned to users. Through these 12 roles, a total of 185 fields are viewable or editable. The role with the most access to the system, security manager, allows users to edit 154 fields and view all of the 185 fields within the system. The role with the least access, clearance viewer, allows the user to view six fields, while the other roles allow varying levels of access between these two extremes. These roles were designed through a collaborative effort involving DFS managers and the system contractor, and the roles designed are detailed within the system security plan.

OIG's analysis of roles and their associated screens and fields showed that some fields allowed too many roles to access the information. According to the security plan and DFS managers, only the guards, facility security personnel, and Security Branch Chief need access to badge information, however IPSS allows the drug manager and drug tester roles to view and edit this information.

In addition, IPSS users were assigned roles inappropriately based on their job functions. A security guard, who is responsible for issuing temporary badges to employees and visitors, had the highest level of access to IPSS. This level of access was designed for the DFS managers and only two other users have this access; they are both DFS managers. Furthermore, the role designated for senior adjudicators has been inconsistently applied to those who have that job responsibility. One senior adjudicator has the appropriate role, while another senior adjudicator has only the basic

adjudicator role. In addition, there is a role in IPSS designed to allow users only to view clearances, yet this role has not been assigned to anyone. Furthermore, although the drug testing module is not currently functional, two IPSS users have been inappropriately assigned the drug tester and drug manager role. One facility staff member has been assigned both the drug tester and drug manager role and a processor has been assigned the drug tester role.

No Audit Trails

IPSS does not contain functional audit trails and the system lacks the ability to allow managers to track user activity and identify misuse of the system. Although audit trails were required for inclusion in IPSS, DFS opted not to pursue this security measure. Managers recalled that the contractor expressed that adding audit trails would be difficult and very costly. Although IPSS contains some database level audit trails, this function is not used because it slows down the system to an unworkable level.

Integrity Statement Not Used

The lack of audit trails is compounded by the fact that users are not required to sign an integrity statement acknowledging appropriate use of the system.

Oversight Is Ineffective

IPSS security measures are inadequate because DFS managers performed ineffective oversight of role implementation and assignment. In addition, managers are unaware of the risks posed by a lack of audit trails and failure to use an integrity statement.

IPSS roles allow users to have too much access to the system because quality review procedures have been inadequate. After the contractor delivered the designed roles, the IPSS administrator reviewed the roles to ensure that the access was correct. In addition, when new fields are added to IPSS the system administrator is responsible for establishing what roles should be allowed access. These procedures were not successful to ensure the roles had the appropriate access. Furthermore, DFS managers do not perform periodic reviews on the role assignments to ensure that users have the appropriate roles.

IPSS lacks an audit trail capability because DFS managers were unaware of the risk to the system without this technical security measure. The system contractor stated that creating audit trails would be a complicated process and DFS managers made the decision not to pursue creating audit trails within the system. DFS managers made this decision based on the projected cost to develop audit trails and because their office is small and they felt that the potential for harm to the system is minimal. DFS managers were unaware of the need for an integrity statement, although it is mentioned within the security plan.

Personnel Security Information Is At Risk

Personnel security information is at risk because appropriate security measures over access to the system and its data are not in place to prevent misuse. Some users have too much access to IPSS information, which increases the risk to the quality of the IPSS data. The risk to the data is compounded because there are no measures in place to ensure users are using the system appropriately.

Recommendations

OIG recommends that the Executive Director for Operations:

11. Redefine IPSS user roles in accordance with least privilege requirements.

12. Review role assignments annually and make appropriate adjustments.

13. Add audit trail capabilities to IPSS.

14. Review audit trail reports monthly to ensure appropriate use of IPSS.

15. Require future IPSS users to sign an integrity statement before being granted access to the system. Also require existing users to sign an integrity statement.

E. IPSS LACKS RECORDS DISPOSITION SCHEDULE

IPSS lacks a records disposition schedule because OIS failed to inform DFS of this need during the system development process. As a result, the system is not in compliance with Federal records retention requirements.

Records Disposition Requirements

All Federal records require a records disposition schedule which defines the actions that must be taken when the records are no longer needed for Government business. All disposition schedules must be approved by the National Archives and Records Administration (NARA). Personnel security clearance records are covered by NARA General Records Schedule 18-22a, which states that the paper files need to be destroyed when an employee or contractor dies or not more than 5 years after the employee separates from an agency or the contract relationship expires.

Electronic records are covered by General Records Schedule 20-3a, which states that electronic versions of records scheduled for disposal under the personnel security requirements are to be deleted after the expiration of the authorized retention period for the paper records, or when no longer needed, whichever is later.

No IPSS Records Disposition Schedule

DFS lacks a records disposition schedule for IPSS. A DFS manager explained that even though the paper records must be destroyed, it is useful to retain electronic records because there are occasions when employees or contractors return to NRC after 5 years and it is useful to have a historical record when adjudicating these individuals for clearance or access. The manager was unaware that a records disposition schedule was needed.

When asked to elaborate on what DFS needs to do to ensure compliance with Federal records retention requirements, an OIS records manager explained that DFS must develop a schedule and process for IPSS records disposition that is worked into its operating procedures and into an IPSS user guide.

DFS Was Unaware of Requirement

IPSS lacks a records disposition schedule and associated implementation plans because OIS failed to inform DFS of this need during the system development process. According to an OIS manager, the need for a records disposition schedule would

typically be identified when an office first approaches OIS to begin planning for a system. The manager said there are measures currently in place to ensure that these steps occur.

NRC Is Noncompliant With Records Requirement

Without an IPSS records disposition schedule and a process to ensure it is followed, NRC is not in compliance with Federal records retention requirements.

Recommendations

OIG recommends that the Executive Director for Operations:

16. Develop a records disposition schedule for IPSS and incorporate it into DFS procedures and the IPSS users manual.

F. SIGNIFICANT ISSUES REMAIN

It has been more than 2 years since IPSS was deployed by DFS for routine use in support of the agency's security programs, yet significant problems remain. These problems pertain to the system's lack of functionality, inaccuracies in system data, missing system checks, and ineffective security measures, which, taken together, jeopardize the agency's ability to efficiently manage its personnel and facility security programs.

The contract to develop IPSS is now in its seventh modification and DFS managers anticipate that up to $90,000 more will be needed to finish developing the system by a new target date of December 2006. Given the previous complications in fulfilling the system design requirements, there is no assurance that the system will perform satisfactorily even 1 year from now.

OIG recommends that the Executive Director for Operations:

17. Conduct a cost-benefit analysis to determine whether the agency should continue to develop IPSS versus replacing the system. As part of the cost-benefit analysis consider current Federal personnel security requirements.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

1. Assign an Office of Information Systems project manager to work closely with DFS for the remainder of the IPSS development process.

2. Correct the reinvestigations notifications report so that all overdue cases are identified and submitted for reinvestigation.

3. Develop and implement a consolidated data entry guide for IPSS users and update it every 6 months or as needed.

4. Review and correct the most recent reinvestigation dates within IPSS.

5. Change IPSS to eliminate the requirement to duplicate clearance data within the system.

6. Eliminate data that was purposely duplicated as a workaround in IPSS records for individuals with a clearance.

7. Perform top-to-bottom cleanup effort of every active file; support this effort with clear written guidance as to what data goes in what field.

8. Develop and implement an overall quality control approach to ensure continued data accuracy.

9. Fix the planned controls to prevent incorrect badge issuance and incorrect clearance assignment.

10. Add date logic controls to ensure that OPM investigation dates follow in logical chronological order.

11. Redefine IPSS user roles in accordance with least privilege requirements.

12. Review role assignments annually and make appropriate adjustments.

13. Add audit trail capabilities to IPSS.

14. Review audit trail reports monthly to ensure appropriate use of IPSS.

15. Require future IPSS users to sign an integrity statement before being granted access to the system. Also require existing users to sign an integrity statement.

16. Develop a records disposition schedule for IPSS and incorporate it into DFS procedures and the IPSS users manual.

17. Conduct a cost-benefit analysis to determine whether the agency should continue to develop IPSS versus replacing the system. As part of the cost-benefit analysis consider current Federal personnel security requirements.

V. AGENCY COMMENTS

At an exit conference held on December 22, 2005, NRC officials generally agreed with the report's findings and recommendations and provided comments concerning the report. In addition, they stated that they were aware of problems with IPSS prior to receiving the draft report. We modified the report as we determined appropriate. 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

Auditors reviewed IPSS to determine if the system meets its required operational capabilities.

The OIG audit team reviewed relevant criteria, including Management Directive 12.3, "NRC Personnel Security Program"; OMB Circular No. A-123, "Management's Responsibility for Internal Control"; OMB Circular No. A-130, "Management of Federal Information Resources"; NUREG-0910, "NRC Comprehensive Records Disposition Schedule"; and NARA's "General Records Schedule." The audit team also reviewed system documentation, including the IPSS contract, security plan, project plan, training plan, data conversion plan, contingency plan, and users guide.

Auditors interviewed DFS and other Office of Administration staff responsible for the system to understand the development and management of the system. Auditors interviewed IPSS users, including adjudicators, facility security staff, processors, and security guards to determine user satisfaction with the system. Auditors also interviewed OIS staff to learn about support OIS should provide to IT system development projects and about agency records retention policy.

Auditors compared information from the paper personnel security records to the corresponding data within IPSS to assess the accuracy of IPSS information and whether the system was capturing individuals due for reinvestigation. Auditors reviewed a total of 262 personnel security files for both NRC employees and contractors. Auditors also conducted tests of the live and production versions of IPSS to assess system data controls.

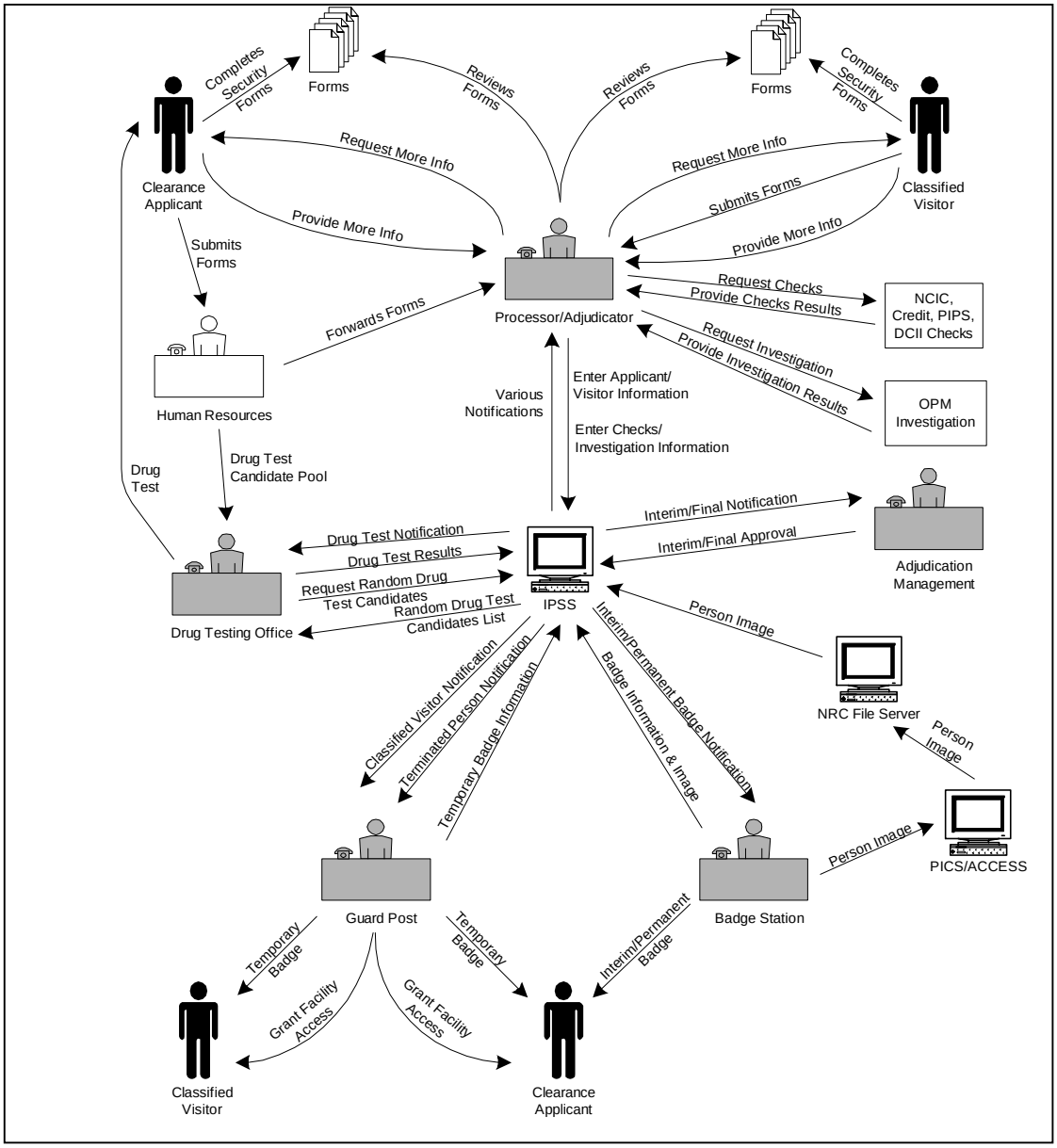
This work was conducted from May 2005 through October 2005, in accordance with generally accepted Government auditing standards and included a review of management controls related to audit objectives. The work was conducted by Beth Serepca, Team Leader; Judy Gordon, Audit Manager; Rebecca Underhill, Management Analyst; and Christopher Lange, Summer Intern.

[Page intentionally left blank.]

Appendix B

DETAILED IPSS DESCRIPTION

The following chart, which appears in the contractor's IPSS design review document, illustrates how IPSS was intended to be used within NRC.



The IPSS Overall Project Plan, dated February 2003, described the following objectives for IPSS:

The objective of this project is to develop an efficient, accurate, and reliable system that meets its functional requirements and replaces the current personnel security software. The IPSS will

- track all personnel security processing activities related to the approval or denial of an employment clearance and access authorization;
- track unescorted contractor access to NRC facilities;
- track due process procedures (denial, revocation, suspension and termination of employment clearance or access authorization);
- provide reporting capabilities;
- track outgoing visits of NRC employees;
- provide a "tickler" system to alert staff when follow-up action is required;
- provide data input along with the images of staff to serve as a badging verification system;
- provide for data consistency, confidentiality, integrity and authentication;
- promote efficient data sharing by consolidating personnel security activities into one integrated system;
- track drug testing activities;
- provide random selection and tracking of drug program participants;
- provide multiple drug testing reports;
- generate standard memos approving or denying access letter authorizations;
- generate email capability to notify facility security staff of access authorizations; and
- provide Ad Hoc reporting capabilities.

IPSS will promote more efficient data sharing by consolidating personnel security activities into one integrated system.