DOE/IG-0548

AUDIT REPORT

PERSONNEL SECURITY CLEARANCES AND BADGE ACCESS CONTROLS AT DEPARTMENT HEADQUARTERS

MARCH 2002

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

U. S. DEPARTMENT OF ENERGY
Washington, DC 20585

March 26, 2002

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Audit Report on "Personnel Security Clearances and Badge Access Controls at Department Headquarters"

BACKGROUND

Security clearances are granted to ensure that only those who have successfully passed a background investigation and have a need to access classified information are actually authorized such access. Security badges provide the physical evidence that a clearance has been granted, and are used by the Department of Energy (Department) to control access to classified information as well as to Departmental facilities and buildings. Currently, about 11,000 badges are issued to Federal and contractor employees working in Department Headquarters. Approximately 4,900 of these badges have been issued to individuals who have security clearance to access classified matter and the rest were issued for "Building Access Only" to individuals who do not require a security clearance.

Data pertaining to security clearances and badges for individuals employed at Department Headquarters, both Federal and contractor, are maintained in two separate information systems managed by the Office of Security's Headquarters Security Operations. The Central Personnel Clearance Index system tracks active security clearances, while the Badge Control System tracks all employees' badge levels, expiration and recovery dates, and employer information. An important function of the Badge Control System is to assist security guards in determining an individual's employment status, badge level, and access authorization in the event that the employee arrives at work without a badge.

In our Special Report on *Management Challenges at the Department of Energy* (DOE/IG-0538, December 2001), we noted that maintaining adequate security and safety continue to be among the most difficult challenges facing the Department and we identified specific security controls that needed to be strengthened. You also underscored the importance of observing the highest standards of security in your October 2001 message on the Department's mission and priorities. In this vein, the objective of our audit was to determine whether the Department terminated unneeded security clearances and recovered unneeded badges.

RESULTS OF AUDIT

Our limited review disclosed that, due to process problems with the Department's clearance and badging controls, unauthorized individuals could gain access to Department Headquarters. Consequently, rather than expand our review to more precisely gauge the scope of the problem,

we truncated our audit and elected to immediately inform management of our findings. Of 147 Federal and contractor employee records selected for initial review at Headquarters, in nine cases, despite discontinued employment, the Department had either not terminated the employees' clearances or had not recovered their badges.

While we found no instances of inappropriate access, these errors, which could have allowed unauthorized individuals easy entry to Department facilities, occurred because program offices did not always provide necessary employment information to Headquarters Security Operations. Additionally, program offices did not always hold contractors accountable for adherence to Department policy regarding clearance termination and badge recovery. Any delay in terminating unwarranted clearances or badges raises concerns regarding the vulnerability of Department facilities, property, classified materials, and the safety of it workers.

We recommended that the Office of Headquarters Security Operations expeditiously review, and correct as necessary, all data in the Department's clearance and badge control systems. We also recommended a number of system enhancements to improve communication among program offices, Headquarters Security Operations, and the Department's clearance-related information systems.

MANAGEMENT REACTION

The Office of Headquarters Security Operations agreed with our recommendations and planned to take corrective actions.

Attachment

cc: Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Chief of Staff
Director, Office of Security

PERSONNEL SECURITY CLEARENCES AND BADGE ACCESS CONTROLS AT DEPARTMENT HEADQUARTERS

TABLE OF CONTENTS

OVERVIEW

INTRODUCTION AND OBJECTIVE

Personnel security measures ensure that individuals have access authorization commensurate with their official duties. Building access is granted to Federal and contractor employees to enable them to enter Department of Energy (Department) facilities to perform their work. Access to classified matter is granted to employees only when their official duties require such access, and only when it has been determined that such access is consistent with national interests. Further, the Department should maintain the numbers and types of access authorizations at the minimum levels necessary.

Access to facilities and classified information is controlled with security badges. According to an official of the Office of Security's Headquarters Security Operations, Department Headquarters currently has about 11,000 badges issued to Federal and contractor employees. Approximately 4,900 of the badges have been issued to individuals who have a security clearance to access classified matter. The Department grants three primary types of security clearances and/or badges:

- "Q" clearances permit access to top secret restricted and formerly restricted data, and national security information.

- "L" clearances permit access to confidential restricted data, secret formerly restricted data, and national security information.

- "Building Access Only" (BAO) badges are issued to individuals who do not require a security clearance. The BAO badge permits access to Departmental facilities.

Data pertaining to security clearances and badges for individuals employed by the Department and its contractors are maintained in two separate information systems managed by Headquarters Security Operations. The Central Personnel Clearance Index (CPCI) system tracks security clearance information such as clearance status, level, and investigation dates. The Security Badge Control System (Badge Control System) tracks individual badge levels, expiration and recovery dates, and employer information. The Badge Control System contains information on all employees regardless of their badge level. The guard force uses this system to confirm badge status and level for anyone who comes to work without a badge.

We initiated this review to determine whether the Department terminated unneeded clearances, recovered unneeded badges, and conducted timely reinvestigations. Our limited review of the timeliness

of the reinvestigation process found no significant backlogs. This report, therefore, focuses on whether the Department terminated unneeded clearances and recovered unneeded badges.

CONCLUSIONS AND OBSERVATIONS

Of 147 Federal and contractor employee records judgmentally selected for initial review at Department Headquarters, we determined that in nine cases, the Department had either not terminated the employees' clearances or had not recovered their badges. In three of these instances, the Department's data systems indicated that the individuals held Q clearances, the highest clearance granted, even though all three had no continuing business with the Department. The remaining six were shown as having badges granting access to Department facilities even though they, too, were no longer employed by the Department or its contractors.

These errors that, in essence, could have allowed unauthorized individuals easy access to Department facilities, occurred because program offices did not always provide necessary employment information to Headquarters Security Operations. Additionally, program offices did not always hold contractors accountable for adherence to Department policy regarding clearance termination and badge recovery. When clearances and badges are not promptly terminated, risks to Departmental facilities, property, classified materials, and the safety of its workers are increased.

Our initial review disclosed that unauthorized individuals could gain access to Department Headquarters. We, therefore, elected to inform management of our findings immediately, rather than to expand our review to more precisely gauge the scope of the cited problems. We are recommending that the Office of Headquarters Security Operations expeditiously review, and correct as necessary, all data in the Department's clearance and badge control systems. We are also recommending a number of system enhancements to improve communication among program offices, Headquarters Security Operations, and the Department's clearance and badging information systems.

Previous Office of Inspector General reports have also cited security control weaknesses. In our 1986 report on *Retention of Security Clearances at Department of Energy Headquarters* (DOE/IG-0228, July 1986), we noted that security clearances for more than one-third of individuals no longer affiliated with the Department had not been terminated and responsibility for clearance termination was not clearly

defined. Based on that finding, we recommended that the Department 1) develop an interface between the personnel and security automated systems to identify individuals with security clearances who have terminated employment or transferred; 2) clarify program office responsibilities, and the procedures and timeframe for terminating clearances; and 3) coordinate with the Department's Procurement office to ensure that standard provisions on clearances are included in contracts and that procedures are developed for terminating clearances as a part of the contract close-out process. Although certain corrective actions were taken, some of the recommendations in the 1986 report still have not been fully implemented. Complete implementation of these recommendations may have prevented some of the examples disclosed during our current audit.

More recently, we reported in 1993 that clearances were granted to individuals who did not require access to classified material, and that there were delays in clearance requests and reinvestigations Department-wide, although Headquarters' processing times were found to be within prescribed goals (*Review of DOE's Personnel Security Clearance Program***,** DOE/IG-0323, March 1993). A 1999 review of the Department's audit follow-up process disclosed that although the total number of clearances had been reduced, there were still delays in processing clearance requests and reinvestigations Department-wide (*The U.S. Department of Energy's Audit Follow-Up Process***,** DOE/IG-0447, July 1999). Appendix 2 lists additional related audit reports.

Management should consider the issues identified in this report when preparing its year-end assurance memorandum on internal controls.

(Signed)
Office of Inspector General

Clearance Termination and Badge Recovery

From lists of contractor and Federal employees provided by the Department's Corporate Human Resource Information System, the Badge Control System, and certain program offices, we selected clearance and badge records for 35 contractor and 112 former Federal employees for initial review. As illustrated in the following table, we confirmed a total of nine discrepancies where former Federal and contractor employees, although no longer associated with the Department, remained active in the CPCI and/or the Badge Control System, permitting potential access to Department facilities and sensitive information.

Contractor and Federal Employees

No. of Employees Selected for Review	No. of Discrepancies Noted	Type of Discrepancy *			
		Active Q Clearances in CPCI	Active Q in Badge System	Active BAO in Badge System	Badges Not Recovered
Contractor-35	6	3	2	3	5
Federal-112	3		1	2	3

*Some employees had more than one type of security clearance/badge discrepancy.

As illustrated above, the Department's data systems showed that six former contractor employees inappropriately retained Q clearances, security badges, or both. Three of these individuals were listed as holding Q clearances, which can allow the highest level of access to facilities and information the Department grants. We were able to contact two of the Q-cleared former contractors and confirmed that neither had any continuing business with the Department. One had been retired for over a year and reported to us that he still had his Q badge. The other individual confirmed that he had no need for any further contact with or access to the Department. This individual also said he had returned his badge to the program office for which he previously worked. However, according to the Badge Control System, the badge had not been recovered.

Additionally, three former contractor employees were listed as having active BAO badges that allowed access to Department buildings. For each of these instances, we confirmed that the individuals were no longer working for the program office listed in the Badge Control System and that badges had not been returned to Headquarters Security Operations.

From our selection of 112 former Federal employees, we found one instance where an individual retired for more than a year was listed in the Badge Control System as having a valid Q badge. The program office confirmed that, after the employee had retired, they did not properly return the badge to Headquarters Security Operations. In two other cases, terminated Federal employees were listed as having valid BAO badges.

It should be noted that erroneous information in either the CPCI or the Badge Control System could result in unauthorized access to Department facilities and information. Even without a badge, a person who is listed in the Badge Control System can gain access to a Department facility. We confirmed this by reviewing procedures with security personnel who told us that if a person presented a driver's license or similar identification and was listed in the Badge Control System, he or she would be issued a temporary badge and granted immediate access. Thus, the accuracy of both the CPCI and the Badge Control System is a critical security control.

Based on the discrepancies we found in our initial selection, our analysis of program office and Headquarters Security Operations procedures, and our follow-up discussions with former employees, we concluded that at least some unauthorized individuals could have gained access to the Department had they chosen to do so. While we have no indication that any unauthorized access actually occurred, we elected to inform management of our findings immediately, rather than to expand our review to more precisely gauge the scope of the cited problems. Headquarters Security Operations agreed to eliminate the discrepancies in the CPCI and Badge Control Systems based on this finding.

Clearance Termination and Badge Recovery Procedures

Chapters IV and X of the Headquarters Facilities Master Security Plan (Plan) outline the procedures and program office responsibilities for Department security clearances and badges required for facility access.

Chapter IV states that Department security badges are the property of the Government and must be returned to the badging office whenever an individual is transferred, terminates employment, or otherwise no longer requires the badge. Chapter X requires program offices, including managers, security officers, and Contracting Officers' Representatives, to ensure that security clearances for those individuals no longer requiring an access authorization are terminated. A Security Termination Statement must be signed by both the individual who no longer requires access authorization and the program office representative. For departing Federal employees, an Employee Separation Clearance form is used to ensure that all property, including security badges, is returned to the Department. Specific program office responsibilities in Chapters IV and X state that program offices are responsible for ensuring that clearances are terminated and badges are returned to the badge office. In addition, both chapters state that contractors that fail to return Department badges from their employees who no longer require the badge could be subject to administrative action that may adversely impact the contract.

A Secretarial Policy Statement on security incidents and violations was issued on June 17, 1999, to improve individual and management contract accountability. Specifically, it enforces a "zero tolerance" policy for Federal and contractor employees who disregard security policies and requirements contained in the Plan. In addition, it states that contracts must require compliance with Department Order 470.1, Safeguards and Security Program, and that contract clauses are to be developed to put performance fees at risk when contractors do not achieve satisfactory ratings in accordance with the Plan.

Information Exchange and Contract Oversight

Clearances were not terminated and badges not recovered because program offices did not always provide information regarding employee status to Headquarters Security Operations. In addition, program offices did not impose contractual controls that would have ensured proper security performance.

Information on Employee Status

Our audit disclosed an absence of up-to-date information regarding some contractor employees. According to Headquarters Security Operations, the security data systems were not updated because program offices did not provide information on employee status. Even

within program offices, information was not always communicated to those who needed it. Contracting Officers' Representatives told us that contractors do not always notify program offices when an individual's employment status changes. As a consequence, neither the Contracting Officer's Representative nor the security officer can initiate appropriate action to recover the badge, terminate the clearance, or inform Headquarters Security Operations of the change. Furthermore, departing contractor employees are not required to complete an Employee Separation Clearance form, which would facilitate recovery of the badge. The result is that some contractor employees leave but necessary changes are not made to the CPCI and the Badge Control System.

As part of our analysis, we asked security officers representing 10 program offices to provide a list of contractor employees who terminated their employment during Fiscal Year (FY) 2001. After numerous unsuccessful attempts to obtain the data, we concluded that the information was not readily available. Only the Offices of Environmental Management, Science, and Defense Programs provided lists that were generated from their own databases. However, Defense Programs and Environmental Management indicated that their lists could be incomplete because they did not include contractor employees who may have terminated without their knowledge. One program office told us that it could not account for contractor employee status. Without such accountability, program offices will continue to be unable to provide up-to-date information on security clearances and badges.

With regard to two of the three former Federal employees noted as exceptions, program offices had not provided updated information to Headquarters Security Operations. Furthermore, there was no interface between the Corporate Human Resource Information System, which tracks Federal employment status, and the Headquarters Security Operations' CPCI and Badge Control Systems. This interface could have provided Headquarters Security Operations with information about the terminations as soon as it was entered into the Corporate Human Resource Information System.

Contractual Controls

Program offices did not always impose controls to hold the contractors and their employees accountable for incomplete security procedures

and unreturned badges. Only one program office we reviewed, for example, associated negative performance fees with unreturned badges. The security officer in this case told us that he has no problems getting the badges back and has, in fact, recovered 100 percent of badges from terminated contractor employees. If contractor security performance is not linked to contract performance fee in this manner, there may not be sufficient incentive for contractors to provide the Department with essential employee status information in order for security procedures to take place.

Risks of Unauthorized Access

National Security Information, various types of classified and unclassified property, and the security of Department workers are at risk if security controls are not rigorously enforced. The lapses cited in this report could have allowed unauthorized individuals entry into Department buildings and, within those buildings, access to areas containing classified information. Information and property that is integral to our national security could, therefore, have been at risk. The possibility that disgruntled former employees could gain easy access with the intent to disrupt operations, obtain information, or cause harm to Department property or employees, must also be seriously evaluated and minimized.

RECOMMENDATIONS

We recommend that the Director, Office of Headquarters Security Operations, work with Headquarters program offices and the Office of Human Resources Management to:

1. Evaluate and correct as necessary information on all Headquarters employees in both the CPCI and the Badge Control System to ensure only currently employed individuals have active status.

2. Develop an interface between systems managed by Headquarters Security Operations that track clearances and security badges, and the Office of Human Resources Management system that tracks employment status.

3. Ensure that program offices receive notice when contractor employees leave, and return badges recovered from these employees to Headquarters Security Operations.

4. Establish a policy to strengthen contractual requirements by:

    a. Requiring contractors to hold formal exit briefings for their terminating employees; and,
    b. Placing performance fees at risk on fixed-price and performance-based contracts.

MANAGEMENT COMMENTS

The Office of Headquarters Security Operations concurred with our recommendations and planned to take corrective actions to address the conditions cited in this report.

AUDITOR COMMENTS

Management actions were responsive to the recommendations.

APPENDIX 1

SCOPE

The audit was performed from October 2001 through January 2002 at Department of Energy Headquarters in Washington, DC and Germantown, MD. The universe of our Federal employee sample consisted of individuals terminating their employment in FY 2001. The universe of our contractor sample consisted of a judgmental sample of active contractor employees employed during 2001.

METHODOLOGY

To accomplish the audit objective we:

- Reviewed lists of contractor and Federal employees provided by the Department's Corporate Human Resource Information System, the Badge Control System, and certain program offices.
- Reviewed information contained in both the Badge Control System and the Central Personnel Clearance Index.
- Interviewed officials from the Office of Headquarters Security Operations and selected program office security officers to understand roles, responsibilities, and procedures.
- Interviewed contractors to ascertain status of employees.
- Interviewed terminated employees to ascertain whether they possessed badges.
- Tested the Badge Control System to ascertain if a terminated individual could gain access to the facilities.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. Because of problems with data inputs, we questioned the validity of computer-processed data.

Management waived an exit conference.

APPENDIX 2

PRIOR REPORTS

OFFICE OF INSPECTOR GENERAL REPORTS

- *Retention of Security Clearances at Department of Energy Headquarters,* (DOE/IG-0228, July 9, 1986). Security clearances for more than one-third of individuals no longer affiliated with the Department had not been terminated and responsibility for clearance termination was not clearly defined. It was recommended that (1) data in the Security information system be corrected, (2) procedures be implemented to recertify clearances, (3) interfaces be developed between personnel and security systems to identify individuals with clearances who have terminated, (4) the request for clearance form be modified, (5) clearance provisions be included in contracts and procedures developed to terminate clearances during contract closeout, and (6) responsibilities and timeframes be outlined in DOE Order 5631.2A.

- *Review of DOE's Personnel Security Clearance Program, (*DOE/IG-0323, March 1993). The Department granted clearances to individuals who did not specifically require access to classified material. The field offices did not follow procedures for clearance terminations, justifications, and recertifications. Delays were also found in processing clearance requests and reinvestigations Department-wide, although Headquarters' times were within the goal of 90 days. It was recommended that blanket clearances be discontinued, a critical review of clearance justifications be performed, numbers and levels of clearances be reduced, standards be developed for cases containing derogatory information, and cases be adjudicated within 90 days.

- *The U.S. Department of Energy's Audit Follow-up Process,* (DOE/IG-0447, July 1999). The Department reduced clearances by 32 percent by eliminating blanket clearance policies and scrutinizing requests. Reduction was also attributed to decreased employment level. There was limited success in timely processing of clearance requests and reinvestigations. It was recommended that an action plan be developed to decrease backlogs and delays and that an assessment be performed on decentralized funding for security clearances.

GENERAL ACCOUNTING OFFICE (GAO) REVIEWS

- *Key Factors Underlying Security Problems at DOE Facilities,* (GAO/T-RCED-99-159, April 20, 1999). Over the last 20 years, GAO has continually cited weaknesses in security at the Department. Testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives, provides an overview of GAO's work on various DOE security areas. In particular, problems in the personnel security area date back to the early 1980s. Problems were noted such as performing timely security investigations, inaccuracies in the security clearance database, and employees with clearance badges without active clearances.

IG Report No. : DOE/IG-0548

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.