



U.S. Department of Energy  
Office of Inspector General  
Office of Audit Services

# Audit Report

Management of the Department's  
Personnel Security and Access  
Control Information Systems

# REPORT ON MANAGEMENT OF THE DEPARTMENT'S PERSONNEL SECURITY AND ACCESS CONTROL INFORMATION SYSTEMS

---

## TABLE OF CONTENTS

### **Personnel Security and Physical Access Systems**

Details of Finding .....	1
Recommendations .....	4
Comments.....	5

### **Appendices**

1. Objective, Scope, and Methodology .....	8
2. Prior Reports .....	10
3. Management Comments .....	11



## Department of Energy

Washington, DC 20585

June 18, 2004

### MEMORANDUM FOR THE SECRETARY

FROM:

*Greg Friedman*  
Gregory H. Friedman  
Inspector General

SUBJECT:

INFORMATION: Audit Report on "Management of the Department's Personnel Security and Access Control Information Systems"

### BACKGROUND

The Department of Energy is responsible for ensuring the security of facilities and materials critical to national defense, scientific research, and environmental remediation missions. As such, it maintains numerous information systems to manage personnel security data and to control physical access to sensitive material or areas. As part of the Department's "E Government" initiative, an effort to modernize management processes through greater reliance on electronic systems, the Department expanded the scope of its security clearance processing automated efforts, renaming it the electronic Department of Energy Integrated Security System. The purpose of the new system was to improve processing, sharing, and archiving of clearance information within the Department and with other Federal agencies. The Department also continued to support the Complex Wide Access Control project, an effort begun in 1995, to allow visitors to use their standard security badge across the complex.

For several years, the Office of Inspector General has reported on integration and system development problems encountered by a number of the Department's program offices. We initiated this audit to determine whether the Department had adopted an integrated and cost-effective approach for developing and maintaining personnel security and physical access control information systems.

### RESULTS OF AUDIT

The Department's information systems modernization initiatives were not designed in a manner that would adequately address long-standing economy and efficiency issues related to its personnel security and physical access systems. Specifically, ongoing system development efforts or management initiatives will not:

- Significantly improve the ability of its corporate personnel security system to track visitor site access, reconcile with contractor clearance tracking systems, enable field sites to generate customized reports, or increase user system access;
- Eliminate costly development and maintenance of numerous separate, site-level personnel security information systems; and,



- Reduce overlapping or redundant physical access control systems that do not communicate with each other, including those at some facilities located in close proximity to one another.

Fulfillment of its long-term objectives in this area were at risk because the Department: (i) had not developed a comprehensive framework for modernizing its personnel security and access control information systems, and, (ii) did not always follow sound system development practices. Absent a coordinated approach, the Department is unlikely to achieve its objective to improve the cost-effectiveness and efficiency of these critical systems. In particular, the eight sites we obtained data from have spent or have plans to spend at least \$13 million to develop, implement, or maintain multiple systems that will not significantly improve the management of personnel security and access control processing.

During our audit, officials from the Office of Security told us that they believe their current initiatives will reduce overall clearance processing times and improve effectiveness. In addition, these officials indicated that they have conducted a number of quality panel meetings and have developed a plan to enhance the corporate personnel security system. While these efforts are noteworthy, additional action is needed to improve efficiency at contractor operated sites and reduce physical access system implementation costs. In that light, this report makes several recommendations designed to improve the overall management of personnel security and access control related information systems.

#### MANAGEMENT REACTION

Management concurred with the report's overall conclusion and the intent of the recommendations but did not agree with our recommended approach to resolving these issues. Management believed that a framework was in place, but steps were necessary to institutionalize it and ensure adherence to existing system development policies. Nevertheless, management agreed to work together with multiple program offices and the Office of Management and Budget to address the issues discussed in this report.

While management's proposed actions are positive steps, the root cause of the issues discussed in the report is the lack of a comprehensive framework and coordinated approach to developing and maintaining security related information systems. Without a comprehensive approach that addresses and resolves basic corporate system access and functionality issues, it is likely that the Department and its contractors will continue to develop duplicative systems, with all the attendant consequences of such duplication.

Management's comments are summarized beginning on page 4 of the report and are included as Appendix 3.

Attachment

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

# PERSONNEL SECURITY AND PHYSICAL ACCESS SYSTEMS

---

## System Modernization Integration, and Development

While the electronic Department of Energy (Department) Integrated Security System (eDISS+) in place at the time of our review may ultimately improve personnel security processing, the initiative was not designed to, and will not address, many of the functionality and access issues reported by a number of sites. Specifically, Central Personnel Clearance Index (CPCI) enhancement efforts will not include a number of site-level needs and will not reduce or eliminate the dependence on separate, locally developed and maintained tracking systems. In addition, the effort to improve physical access control systems was not well organized and lacked the capability to reduce duplicative and overlapping system development efforts.

### Clearance Tracking Systems

Although the Department plans to make further enhancements to CPCI, planned modifications will not address a number of site-level needs. Originally deployed in 1968, CPCI is used to maintain clearance data for Federal and contractor employees. However, according to site officials, it lacks a number of functions needed to effectively manage such information. Specifically, contractor officials told us that the current initiatives to enhance CPCI will not track special or temporary access authority (such as those required for nuclear material handling); provide electronic reconciliation with site-level personnel security tracking systems; or enable field sites to generate customized security reports.

Planned upgrades to CPCI will also not increase access or enhance processing capabilities for contractor operated facilities. For example, contractors at a number of sites will not be granted sufficient access to make electronic updates to CPCI, requiring manual update processes to be used. Clearance terminations will continue to be made by methods such as "hand delivery" or faxing various forms to responsible Federal officials. As we observed in our report on *Personnel Security Clearances and Badge Access Controls at Selected Field Locations* (DOE/IG-0582, January 2003), manual termination methods tend to be more labor intensive, are susceptible to errors based on timing differences, and can increase the risk that individuals will gain access to sites even though their association with the Department has ended.

---

Responsible Headquarters personnel told us that they understood site concerns regarding CPCI and that they were aware of cost and data reliability issues associated with the use of manual methods. Nevertheless, the Department planned to support the CPCI in its present form and continue to restrict contractor access to the system. While Headquarters officials indicated that they permitted contractors to modify CPCI when serving under direct supervision at Federal locations, they believed that extending access to contractor personnel in private company locations could affect data integrity. In subsequent discussions, Headquarters officials clarified their comment and indicated that they did not want to expand access to contractor personnel at government-owned and contractor operated facilities. Headquarters system owners indicated that the information contained in CPCI was highly sensitive and that data entry functions could not be directly entrusted to contractors. These officials maintained their position even though they acknowledged that contractors maintain the same data in local systems and understood that system level protections were available.

The current modernization effort also will not address longstanding problems with duplicative and redundant development and maintenance of site-level security information systems. Specifically, Headquarters security officials indicated that sufficient resources do not exist to resolve CPCI functionality and access issues discussed above. Accordingly, contractors at each major site told us they must continue to develop and maintain separate, but functionally equivalent personnel security systems. We noted that problems with duplicate development have not improved substantially since we reported the issue in our 2000 report on *Corporate and Stand-Alone Information Systems Development* (DOE/IG-0485, September 2000). For example, our review disclosed that each of the eight sites we visited or obtained data from had developed and were maintaining a separate clearance tracking system. Officials from the National Nuclear Security Administration (NNSA) Service Center in Albuquerque told us it cost over \$660,000 to develop and maintain its personnel security system.

---

## Access Control Systems

Our audit disclosed that the Department maintains a number of duplicative and overlapping physical access control systems. Such systems, designed to limit or control access through electronic, mechanical, or biometric means, are used to protect sensitive material and sites across the complex. The Department's current effort to improve physical access control systems will not reduce duplicative and overlapping system development or increase the ability to share data between these systems.

The Complex Wide Access Control (CWAC) project was designed to provide a capability to allow sites to retrieve fundamental information regarding Department and contractor employees visiting Departmental sites. However, it lacked the capability to reduce duplicative overlapping system development that is occurring at the field sites. Furthermore, the project has not been well defined. Even though the CWAC project has been in planning or development since 1995, the Department has not yet determined which sites will use it or how implementation will proceed. In particular, while the sites we visited were aware of the project, none understood the cost and schedule for implementation. In addition, we learned that a cost-benefit analysis had not been conducted and, despite a number of changes in scope and schedule, the project plan had not been adequately updated. Had CWAC been incorporated into the Department's E-government initiative, it may have focused the development and deployment effort, helped increase integration, reduced the number or type of separate physical access control systems, and increased the return on the \$3.5 million invested in the project to date.

Even when in close proximity to one another, sites chose to operate independent access control systems. For example, until recently, Oak Ridge Reservation sites shared the same access control system. However, in 2001, Oak Ridge National Laboratory (ORNL) installed its own separate access control system that uses proximity cards. Meanwhile, the Y-12 Complex (Y-12) is considering replacing its access control system – which is shared by the East Tennessee Technology Park – and may also use proximity cards. However, responsible Y-12 officials we spoke to had no plans to integrate this system with ORNL's new access control system. Additionally, Los Alamos National Laboratory, Sandia National Laboratories, and the NNSA Service Center each

---

maintained independent access control systems despite constant interaction among personnel assigned to the sites. Thus, frequent and cumbersome reconciliations were necessary to ensure appropriate access to these sites.

**Security Information Systems Approach**

Efforts to modernize and improve the efficiency of personnel security and physical access control systems were at risk because the Department had not developed a comprehensive security systems framework. Specifically, the Department had not determined the most effective method to manage personnel security and physical access across the complex. No central authority had been established and no organization had taken the initial step of developing a framework by identifying the universe of personnel security and access control systems and their associated costs. As we have noted in prior reports, absent a comprehensive framework to guide systems development activities, there is no mechanism to ensure that systems being developed are not duplicative or redundant and are able to communicate with one another. In addition, as we noted in the development of physical access control systems, the Department did not always apply sound project management practices such as cost-benefit analyses or the maintenance of up-to-date project plans for systems development initiatives.

**Costs and Security Risks**

The Department spent or plans to spend at least \$13 million to develop, implement, or maintain multiple systems that duplicate functionality and are not adequately integrated. This includes over \$5 million for the separate access systems development efforts at the Oak Ridge Reservation. Without a comprehensive plan, the Department may be unable to restrict future duplicative development efforts or improve the cost-effectiveness and reliability of its security systems. Additionally, the lack of systems integration increased the risk that sites would grant access to unauthorized individuals based on ineffective or untimely information updates.

**RECOMMENDATIONS**

We recommend that the Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration, in conjunction with the Director, Office of Security and Safety Performance Assurance and the Chief Information Officer:

1. Develop a comprehensive framework for managing and integrating personnel security and access control systems Department-wide by:

- 
- a) Determining the universe of personnel security and access control systems across the complex and the costs associated with operating and maintaining these systems; and,
  - b) Developing and implementing a plan, based on data gathered and an assessment of corporate systems capabilities, for ensuring that personnel security and access control systems are not duplicative, have the ability to share data, and will provide maximum benefit to the Department.
2. When selecting, developing and implementing future personnel security and access control systems, require that organizations comply with existing Office of Management and Budget (OMB) and other established standards and policies related to capital investment, project management and systems development. Specifically, ensure that all efforts include elements such as cost-benefit analyses, project plans, critical decisions and senior management oversight and approval.

**MANAGEMENT  
REACTION**

Management generally concurred with the report's overall conclusion and the intent of the report's recommendations. Management agreed that dependence by sites on duplicative, locally developed systems hampers efficiency and is not cost effective. However, management disagreed that the problems in this report derive from the Department's lack of a comprehensive framework for its personnel security and access control systems. Management also believed that the report should have emphasized the need for compliance with the Department's existing policies and procedures and OMB regulations regarding information systems planning, acquisition, development, and management. Management further indicated that the risk of expanding access to CPCI outweighs any potential cost or time savings. The Office of Security and Safety Performance Assurance also provided a number of technical comments regarding the report.

**AUDITOR COMMENTS**

Management's comments are partially responsive to our recommendations. While we are encouraged that management agrees in principle and plans to address our recommendations, we disagree with its assertion that a framework is in place and that the Department has fielded a complete enterprise architecture. We

---

found the lack of a security framework was a root cause of the problems identified. Specifically, the examples of duplicate and overlapping access control systems contained in this report demonstrate that the Department does not have an agreed upon set of standards or requirements for controlling development of new personnel security and access control systems -- an integral and essential component of a framework for making investment decisions. Establishing a framework that includes a complete enterprise architecture would give the Department the tools necessary to determine how complex-wide needs should be addressed. As noted previously, we have issued a series of reports that highlight the lack of such a comprehensive approach to information technology management.

With regard to management's concern that our report should emphasize the need for compliance with existing Department policies and procedures and OMB regulations, we agree and have made several changes to the report and recommendations to reflect that concern.

We also agree with management's position that the Department needs to maintain strict control over CPCI and grant access only on the basis of a legitimate "need to know." However, the contractors we reference in this report operate Federal facilities, are subject to Federal oversight, and many already have access to sensitive data in order to perform their daily work. As noted in the report, secure contractor access is possible by restricting the level of access or by using batch processing techniques to monitor and control contractor changes. For example, as we discussed with program officials during our audit, batch techniques could eliminate manual processing methods and permit electronic entry of data by contractors while providing Federal officials with the ability to review and approve the data prior to releasing it to the system.

Where appropriate we have incorporated management's technical comments in the body of this report. Management's comments are included in Appendix 3.

# Appendix 1

---

## OBJECTIVE

The objective of this audit was to determine whether the Department had adopted an integrated and cost-effective approach for developing and maintaining personnel security and physical access control information systems.

## SCOPE

The audit was performed between December 2002 and October 2003 at the National Energy Technology Laboratory in Morgantown, WV, and Pittsburgh, PA; the Pittsburgh Naval Reactors in West Mifflin, PA; Departmental Headquarters in Washington, DC, and Germantown, MD; the Oak Ridge Reservation in Oak Ridge, TN; the Los Alamos National Laboratory in Los Alamos, NM; and the Sandia National Laboratories and the NNSA Service Center in Albuquerque, NM. We also obtained information from the Lawrence Livermore National Laboratory in Livermore, CA.

## METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and regulations pertaining to personnel security and access control systems. We also reviewed reports issued by the Office of Inspector General and the General Accounting Office;
- Reviewed the *Government Performance and Results Act of 1993* and determined if performance measures had been established for personnel security and access control systems;
- Reviewed numerous documents related to all personnel security and access control systems in operation or under development at the sites we visited;
- Reviewed documentation pertaining to Department-wide personnel security and access control initiatives, such as the OMB Exhibit 300 budget submission for eDISS+ and the CWAC budget plan; and
- Held discussions with program officials and personnel from Department of Energy Headquarters, including representatives from the Office of the Chief Information Officer, field sites visited, and the Department of Defense.

## Appendix 1

---

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 objectives. Accordingly, we assessed internal controls regarding the management of the Department's personnel security and access control systems. 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. While we examined a number of systems access and control related issues, we did not rely on computer-processed data to accomplish our audit objective.

## Appendix 2

---

### PRIOR REPORTS

- *Management Challenges at the Department of Energy* (DOE/IG-0626, November 2003). The Department continued to experience challenges in a number of important areas, including information technology management and national security. Specifically, the Department had not fully satisfied the requirements of the Clinger-Cohen Act to effectively manage information technology. The lack of a baseline to guide the acquisition and management of information technology resources was one of the significant barriers identified to achieving the objectives of the Clinger-Cohen Act.
- *Personnel Security Clearances and Badge Access Controls at Selected Field Locations* (DOE/IG-0582, January 2003). At three of four field sites visited, minor discrepancies were found in the recovery of badges. However, the fourth site had a significant number of badges that had not been recovered from former contractor and other non-Federal workers. Specifically, the site had not recovered badges for eight percent of the workers included in the sample that had terminated their employment with the Department. These discrepancies occurred because non-automated transmission of the data was not always effective. Further, site badge officials did not always follow up with Department personnel security offices to ensure that the termination information was received and that the clearance system was updated.
- *Personnel Security Clearances and Badge Access Controls at Department Headquarters* (DOE/IG-0548, March 2002). Due to problems with the Department's clearance and badging controls, unauthorized individuals could gain access to Department Headquarters. Specifically, the Headquarters badging system and the Central Personnel Clearance Index contained inaccurate information regarding the status of employee terminations. The inaccuracy of the information could allow unauthorized personnel to enter Department Headquarters facilities and present a risk to national security. The systems contained inaccurate data because program offices did not always provide information regarding employee status to Headquarters Security Operations.
- *Information Technology Support Services Contracts* (DOE/IG-0516, August 2001). The Department was not effectively managing the acquisition of information technology support services. Problems arose because the Department had not developed and implemented a framework for acquiring information technology support services in an efficient and cost-effective manner. As a result, the report concluded that savings of as much as \$44 million may be possible over a three year period by adopting a Department-wide approach.
- *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996* (DOE/IG-0507, June 2001). The Department had not satisfied major requirements of the Clinger-Cohen Act. Specifically, it had not developed and implemented an integrated

## Appendix 2

---

enterprise-wide, information technology architecture. Additionally, it did not acquire information technology related assets in an effective and efficient manner. As a result of these problems, potential operational efficiencies and savings totaling more than \$100 million were possible through better implementation of Clinger-Cohen requirements.

- *Corporate and Stand-Alone Information Systems Development* (DOE/IG-0485, September 2000). The Department had spent at least \$38 million developing duplicative information systems, and redundant computer systems existed or were being developed at nearly all organizational levels within the Department. Specifically, there were 115 separate security applications in place at five of the field sites sampled. The existence of duplicate information systems occurred because the Department had not finalized a conceptual Information Technology Architecture Plan to control development and the plan was only applicable to Headquarters.



**Department of Energy**  
Washington, DC 20585

April 16, 2004

MEMORANDUM FOR GREGORY FRIEDMAN  
INSPECTOR GENERAL

FROM: GLENN S. PODONSKY, SP-1

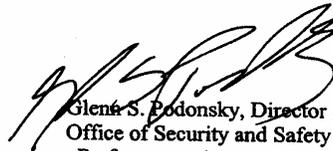
SUBJECT: Consolidated Comments on October 3, 2003, Draft IG Report  
on "Management of the Department's Personnel Security and  
Access Control Information Systems"

The Deputy Secretary requested the Office of Security and Safety Performance Assurance (SSA) to coordinate the Department's response to the subject report. Attachment 1 is a consolidation of comments. SSA concurs with the report's overall conclusion; however, as discussed with your staff, Attachment 2 provides detailed comments on the accuracy and validity of several specific assertions contained in the report.

The Department concurs with the intent of the report's recommendations, but suggests rewording them to state: (1) Institutionalize a framework requiring better compliance with departmental policies, procedures, and guidance related to IT investing by all organizational elements including contractors, laboratories, and field sites; and (2) Enforce the project management requirements documented in DOE Order 413 including critical decisions and senior management oversight and approval for personnel security and access control projects.

The Office of the Chief Information Officer provided significant input to the response that has been incorporated into the body of the Departmental Response (Attachment 1). The Office of Security was the primary lead program in developing the response to this report and also provided extensive comments that are contained in Attachment 2. It may be beneficial for our staffs to meet to discuss the accuracy of several assertions made in the report as well as to collaborate on rewording the recommendations to more effectively address the problems cited in the report before it becomes final.

If you have any questions, please contact Marshall O. Combs, Director, Office of Security at (202) 586-3345.

  
Glenn S. Podonsky, Director  
Office of Security and Safety  
Performance Assurance

2 Attachments

cc: K. McSlarrow, DS  
K. Kolevar, DS Chief of Staff



Printed with soy ink on recycled paper

**Consolidated Comments on October 3, 2003, Draft IG Audit Report  
“Management of the Department’s Personnel Security and Access Control  
Information Systems”**

Headquarters program offices were asked to review and comment on the draft Office of Inspector General (IG) audit report entitled, *Management of the Department's Personnel Security and Access Control Information Systems*. All of the Headquarters' programs concurred without comment to the content and proposed recommendations in the draft report with the exception of the Office of the Chief Information Officer and the Office of Security (SO). The Office of Security was the focal point of the audit and provided several comments on the content that have been incorporated into these comments. Comments provided by the Office of Energy, Science and Environment and the Office of the Chief Information Officer have also been integrated into this document. The Department welcomes the IG recommendations as emphasis on the corporate solution in this important area, and encourages the use of this report as a vehicle of positive change.

The Department agrees with the draft report that dependence by its site offices on duplicative, locally developed systems hampers efficiency and is not cost effective. However, we disagree with the IG's assertion that this problem derives from the Department's lack of a comprehensive framework for its personnel security and access control systems.

The legacy Central Personnel Clearance Index (CPCI), a component of the electronic DOE (Department of Energy) Integrated Security System (eDISS+) is being improved, and the proposed Complex-Wide Access Control (CWAC) system is being implemented at selected sites in the complex. Current local systems that support critical processes at sites need to be carefully integrated into these modernization efforts. The assertion in the draft report that the Central Personnel Clearance Index (CPCI) was not intended to address functionality is inaccurate, however. The current release of CPCI does include programmatic and adjudicative functionality and further enhancements are planned pending funding.

The Department does not believe the potential savings in time derived from allowing contractor employees not subject to Federal oversight access to CPCI, offsets the potential increases in risks posed by possibly reducing control over access to those without a legitimate “need to know.” The CPCI contains sensitive personnel information protected by the Privacy Act and as such, unauthorized access to it represents a significant security risk. The DOE Personnel Security Program has never granted CPCI access to contractor personnel who are offsite in private company locations and does not believe that expediency justifies that change now. The CPCI stores access authorization information that is used by sites to determine whether an individual can be allowed access to classified information and special nuclear material. Thus, the ability to enter the system and add or delete personnel information poses a significant risk to the

Department's classified information and special nuclear material, because the status of an individual as "cleared" or "un-cleared" could be changed with a few keystrokes.

The Department believes the draft report should have emphasized compliance with the Department's policies and procedures addressing information architecture-based planning processes, project management, and Office of Management and Budget circulars pertaining to justification, acquisition, and operation of information systems. These policies and procedures were established to preclude the acquisitions and operations of overlapping and redundant information systems as discussed by the IG in this report.

The IG identified legitimate issues related to the Department's acquisition and operation of overlapping and redundant personnel security and access control information systems. This is not a new problem or a problem that exists only in the area of personnel security and access control systems, but a persistent problem that crosscuts departmental programs and includes all types of information systems. Funding priorities that implement the policies of the Office of Security (SO) and the Office of the Chief Information Officer (CIO) will be crafted with the results of this report in mind.

The IG has reported on this problem repeatedly over recent years resulting in the Department completing several corrective action plans, no doubt costing considerable time and resources. That the IG is reporting this problem again speaks to the complexity of the problem, the inherent difficulty in changing the Department's long standing business practices, and the less than effective results of prior actions. Therefore, coordination between ESE, SO and CIO is vital as the Department moves forward, to ensure that good policy is well executed in the field so that thorough consideration and evaluation of the expected outcome of the recommendations offered in this report is completed and that the subsequent corrective actions address the root causes of this problem. In fact, the Office of Security and the Chief Information Officer are joint members of the new Federal Identity Credentialing Committee. This committee was established by the Office of Management and Budget for the purpose of simplifying and unifying identity authentication for Federal employees; creating requirements for physical credentials, electronic credentials and issuance; and developing the Federal Identity Credentialing component of the Federal Enterprise Architecture. We will work through their committee to accomplish the IG recommendations.

### RECOMMENDATIONS

We recommend that the Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration, in conjunction with the Director, Office of Security and the Chief Information Officer:

**Recommendation 1:** Develop a comprehensive framework for managing and integrating personnel security and access control systems Department-wide by:

- a. Determining the universe of personnel security and access control systems across the complex and the cost associated with operating and maintaining these systems; and,

- b. Developing and implementing a plan, based on data gathered and an assessment of corporate systems capabilities, for ensuring that personnel security and access control systems are not duplicative and provide maximum benefit to the Department.

**Response:** Concur in principle, but non-concur on approach

Suggest rewriting recommendation to state: Many of the elements of a comprehensive framework for managing and integrating personnel security are already in place including a Departmental Enterprise Architecture that includes the security function and an IT capital planning process that requires the elimination of IT investments that duplicate corporate functionality. However, the framework must be institutionalized to better require compliance with Departmental policies, procedures, and guidance related to IT investing by all organizational elements including contractors, laboratories, and field sites.

**Benefits of this Approach:**

This recommendation would lead to a better coordinated personnel security and access control function complex-wide, thus producing an improved security posture for the Department.

**Recommendation 2:** Require that effective project management systems development practices, including preparation of cost-benefit analyses and up-to-date project plans, are followed when selecting, developing, and implementing personnel security and physical access control systems, to include the Complex-wide Access Control project.

**Response:** Concur in principle, but non-concur in approach

Suggest rewording recommendation to state: Enforce the project management requirements documented in DOE Order 413 including critical decisions and senior management oversight and approval for personnel security and access control projects.

**Benefits of this Approach:**

The use of an oversight review for personnel security and access control projects would ensure that all applicable security policy, procedures and guidance are fully implemented as well as ensuring that investments are consistent with EA guidance and capital planning investing goals.

## 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 inspection 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 the 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?
5. 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.