



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

# Audit Report

## Management Controls over the Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2006

OAS-M-06-10

September 2006




## Department of Energy

Washington, DC 20585

September 25, 2006

### MEMORANDUM FOR THE EXECUTIVE DIRECTOR, FEDERAL ENERGY REGULATORY COMMISSION

FROM:

  
Rickey R. Hass  
Assistant Inspector General  
for Financial, Technology and Corporate Audits  
Office of Inspector General

SUBJECT:

INFORMATION: Audit Report on "Management Controls over the Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2006"

#### BACKGROUND

The Federal Energy Regulatory Commission (Commission) has developed and implemented a number of information systems to support its mission of regulating the natural gas industry, hydroelectric projects, oil pipelines, and wholesale rates for electricity. Because of the increasing frequency and sophistication of cyber attacks, the potential for malicious intrusion and damage to these information technology assets and the information they contain continues to grow. During 2006, the Commission estimated that it spent almost \$1 million to protect its \$27 million information technology investment from cyber related threats. The importance of maintaining a robust cyber security program is well demonstrated by the debilitating effects that recent attacks on Federal organizations have had on mission performance, agency reputation, and on constituents that have been subjected to compromise of personally identifiable or sensitive data.

As required by the *Federal Information Security Management Act* (FISMA), and consistent with Congress's desire to develop a comprehensive framework to protect the government's information technology operations and assets, the Office of Inspector General is required to perform an annual independent evaluation of the Commission's cyber security program. This evaluation is designed to assess the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of the FISMA. This memorandum and the attached report present the results of our 2006 evaluation.

#### RESULTS OF EVALUATION

The Commission has continued to strengthen its cyber security program and has completed corrective action on several issues identified during our previous review. In particular, the Commission:



Printed with soy ink on recycled paper

- Improved configuration management procedures by ensuring that software updates were applied and users had only the access privileges necessary to perform their duties; and,
- Enhanced its system for tracking cyber security related corrective actions to resolution.

Although these actions are noteworthy, our evaluation disclosed several opportunities to improve the effectiveness and decrease the risk associated with the Commission's cyber security program. Specifically, we observed that:

- While problems with access controls associated with strong password management had declined since our 2005 evaluation, testing revealed continuing problems with default, blank, or easily guessed passwords, and user account controls; and,
- Security assessments performed in connection with system certification and annual security reviews had not been properly executed or were not adequately documented for each of the four systems we evaluated.

These vulnerabilities existed because the Commission had not ensured that certain aspects of its cyber security program conformed to either Federal or Commission requirements or guidelines. Weaknesses such as the ones we discovered detract from the overall effectiveness of the Commission's cyber security program and potentially expose its information technology resources and data to compromise. As indicated above, we believe that the Commission's overall cyber security posture has improved, however, additional work is necessary to ensure that its information and systems are properly protected from the threat associated with unauthorized or malicious access by insiders. In that connection, we have made several recommendations designed to aid management in achieving that goal.

Due to security considerations, information on specific vulnerabilities has been omitted. However, management officials have been provided with detailed information regarding identified vulnerabilities, and according to management officials, corrective actions have either been completed or initiated.

### MANAGEMENT REACTION

Management concurred with each of our recommendations and indicated that it had taken corrective action to address each of the problems identified in the report. While management recognized that password weaknesses increase the risk of compromise, it did not believe that the problems we identified were significant. We disagree and note that a knowledgeable insider could have exploited the problem passwords – introducing viruses, worms or other malicious programs that could have damaged the Commission's systems. Management's comments and our responses are summarized in the body of our report. Management's comments, in their entirety, are included in Appendix 3.

Attachment

cc: Chief of Staff  
Chief Information Officer, IM-1

# REPORT ON MANAGEMENT CONTROLS OVER THE FEDERAL ENERGY REGULATORY COMMISSION'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2006

---

## TABLE OF CONTENTS

### Cyber Security Program

|   |   |
|---|---|
| Details of Finding .....                      | 1 |
| Recommendations.....                          | 4 |
| Management Reaction and Auditor Comments..... | 4 |

### Appendices

|  |    |
|--|----|
| 1. Objective, Scope, and Methodology ..... | 7  |
| 2. Related Audit Reports.....              | 9  |
| 3. Management Comments .....               | 11 |

# CYBER SECURITY PROGRAM

---

## **Risk Management and Control Procedures**

Our evaluation disclosed that the Federal Energy Regulatory Commission (Commission) had made improvements in its cyber security program and had corrected previously reported weaknesses. Specifically, the Commission improved its configuration management procedures to ensure that only current software versions were used and that user access privileges were restricted to the least level required for job performance. The cyber security corrective action management process had also been modified to ensure that all vulnerabilities and weaknesses were identified and tracked to resolution. In spite of these efforts, several opportunities exist to improve the effectiveness of the Commission's cyber security program as it relates to access controls and security assessments.

### Access Controls

We continued to find that controls over passwords were not always effective. The Commission policy related to passwords requires, among other things, that passwords must be in place for all systems and that they must be unique, difficult to guess, and a minimum length of eight characters. Passwords are a critical element of computer security and provide the basis for controlling access and establishing accountability by identifying and authenticating users. However, our testing revealed that easily guessed, blank, or default passwords existed on several of the Commission's systems. This condition, first reported in our *Evaluation Report on the Federal Energy Regulatory Commission's Unclassified Cyber Security Program-2005* (DOE/IG-0704), continued to exist despite action taken by Commission officials to correct the problem.

In addition, we also observed that controls designed to discover and suspend access for inactive accounts were not always effective. The Commission's Unused Accounts Standard Operating Procedures require that unused network accounts be disabled after 90 days of inactivity to reduce the risk of unauthorized system access. However, our testing revealed that 20 network user accounts remained active even though they had not been used for almost a year. Management explained that delays in removing inactive network accounts were largely due to an

incomplete validation process for the identified accounts prior to their intended disablement. They stated that the validation process involved receiving confirmation from the Commission's Administrative Officers, which had not occurred for the accounts we identified.

### Security Assessments

Security assessments performed in connection with system certification and annual security reviews had not been performed properly or were not adequately documented for each of the four systems evaluated. Annual security assessments, required by Office of Management and Budget (OMB) guidance, determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome. Specifically, the assessments did not evaluate the level of effectiveness of many of the 36 critical control elements specified in National Institute of Standards and Technology (NIST) requirements. Consideration of critical elements, such as those in place to plan for contingencies; to prevent interception of data; and to respond to incidents, had been omitted. For example, one assessment measured the effectiveness of only 2 of the 36 critical elements, while 2 other assessments only measured the effectiveness of 7 and 9 elements, respectively.

We also identified problems with properly preparing and updating assessments prior to re-certification of systems that had previously been provided with authority to operate. For example, management officials told us that, while they had performed the required assessment for one of the agency's systems, they had not documented it and could not provide information necessary for us to evaluate the sufficiency of the procedure. Officials also had not properly updated self-assessments to reflect the required supporting security controls prior to granting systems with continued authority to operate. For one assessment, officials indicated that 61 percent of the required controls were not applicable without explaining why, and in another case either totally excluded or did not explain why 79 percent of the required controls were not necessary.

## **CYBER SECURITY PROGRAM**

---

### **Program Implementation and Oversight**

These vulnerabilities existed, in part, because the Commission had not ensured that certain aspects of its cyber security program conformed to Federal requirements and guidelines. Specifically, continued access control problems were a direct result of configuration controls that were not applied in accordance with the Commission's own requirements and the guidelines set forth by NIST. In addition, the Commission's annual system security review process was not performed in accordance with OMB requirements and did not address all of the critical control elements as defined by NIST requirements.

Information technology management officials told us that, rather than conforming to OMB requirements, they chose to adopt their own approach to certification and accreditation that was better suited to the size and limited resources available to their organization. They believed that after considering the risk associated with their systems, it was appropriate to omit certain steps required by NIST guidance when re-certifying the Commission's systems for operation. Rather than specifically considering each of the NIST-prescribed critical security elements, these officials relied instead on self-assessments performed by system owners, a review and update of the system risk assessment by the certification agent, system owner, and other stakeholders to establish a basis for re-accrediting systems.

While we did not attempt to determine whether departure from NIST guidance was appropriate or advisable in any circumstance, we believe that because of the deficiencies and omissions from the original assessments performed on these systems such approach was not appropriate and increased the risk associated with their operation. As previously noted, many of the 36 NIST-prescribed critical security elements had not been considered when these systems were initially authorized to operate. As such, the assessments did not provide assurance that systems security controls were in place and operating as intended nor did they provide a sufficient basis for the accrediting official to either authorize the system to operate or accept residual risks.

### **Operational Impacts**

Although the Commission's overall cyber security posture had improved, information resources remain vulnerable. As a result, the information and systems that support the



---

Commission's missions and business activities could be at risk of compromise. For example, weak passwords and the failure to identify and disable unused accounts could result in unauthorized access to Commission information resources by malicious users. Inadequate evaluation of system security controls to thoroughly verify the implementation of security controls could also result in undetected information security weaknesses that may hinder the Commission's effort to effectively secure its systems.

## **RECOMMENDATIONS**

Weaknesses identified during the course of our evaluation were discussed with Commission officials and actions were taken to resolve certain problems identified. However, to improve cyber security within the Commission, we recommend that the Executive Director take action to:

1. Ensure that procedures are implemented for securely configuring the Commission's systems by (a) prohibiting the use of easily guessed, blank or default passwords that do not adhere to NIST guidelines; and, (b) correcting systems with improperly configured security settings for various network services;
2. Review and update the procedures relating to unused network accounts to enforce the identification and removal of inactive accounts in a timely manner; and,
3. Ensure that the annual security review processes, used to support the certification and accreditation of systems, thoroughly address the critical control requirements defined by NIST.

## **MANAGEMENT REACTION AND AUDITOR COMMENTS**

Management concurred with our findings and recommendations, but offered clarifying remarks. Management's proposed and stated actions are responsive to our recommendations. In reference to specific comments, management reaction and auditor comments follow:

Recommendation 1: Ensure that procedures are implemented for securely configuring the Commission's systems by (a) prohibiting the use of easily guessed, blank

---

or default passwords that do not adhere to NIST guidelines; and, (b) correcting systems with improperly configured security settings for various network services.

Management Comments: Management stated they confirmed that there were nine accounts identified as having blank or weak passwords. They added that these were local accounts without network access and only two of these accounts provided any elevated privileges to the computer. They also noted that only a small percentage of the Commission's passwords were found to have vulnerabilities.

Auditor Response: We identified a total of 12 blank or weak passwords, including 9 that could have permitted access to the Commission's file servers. Of the nine blank or weak passwords, one of the blank password accounts had an attribute which indicated it was an account with elevated privileges. Two other accounts with blank passwords were system administrator accounts -- accounts highly vulnerable to exploits. As noted by management in their comments, even a small number of accounts whose passwords are not compliant with organizational policy, represent a security issue. For example, gaining unauthorized access via blank or weak passwords could allow a user to compromise systems by installing a trojan, which is a malicious program disguised as or embedded within legitimate software; or a keylogger, which captures the user's keystrokes, providing a means of obtaining unauthorized information.

Management Comment: Management indicated that in order to exploit any of these local accounts, a perpetrator must have either authorized access to the Commission's internal network protected by Microsoft® Active Directory or physical access which would require the circumvention of three increasingly restrictive physical layers of defense, using an authorized badge. They stated that the only way a person without foreknowledge could have discovered the existence of these particular local accounts would be to scan the network and that any internal scanning process would have been detected by the Commission's Intrusion Detection System.

Auditor Response: We agree that these accounts are most vulnerable to knowledgeable insiders – an increasing threat

---

to information technology assets in both Federal and private sector organizations. The audit tests that revealed these password weaknesses were specifically designed to evaluate the "insider threat" associated with an employee or someone who is permitted access to the facility. This scenario assumes the user has network access and that through exploitation of vulnerabilities is able to escalate their assigned level of privileges. Furthermore, although the Commission runs an Intrusion Detection System, exploitation of the vulnerabilities we identified and the infliction of potential damage may have been possible prior to detection by the incident response team.

Recommendation 3: Ensure that the annual security review processes, used to support the certification and accreditation of systems, thoroughly address the critical control requirements defined by NIST.

Management Comment: Management stated they believe they complied with the guidance in NIST SP 800-26 for annual security reviews, but added that they acknowledge that its administrative documentation did not appear to satisfy the IG's definition of acceptable artifacts. They noted they follow system certification and annual security review processes that balance risk and cost and, when appropriate, leverage security assessment activities already performed during the course of the fiscal year. They also stated that these processes incorporate enterprise and system scans, contingency plan testing, and security test and evaluation of technical controls.

Auditor Comment: We are gratified that management, in response to our recommendation, had taken action to complete updates to its self-assessments. Our report does not take issue with the Commission's systems certification and annual security review methodologies. However, as we noted, both the systems certification process and the annual security review process relied on NIST SP 800-26 system self-assessments that failed to consider most of the 36 critical control elements specified in NIST requirements. Reporting guidance for the FISMA, issued by the OMB, requires that annual security reviews be performed in accordance with specific NIST requirements.

Management's comments are included in their entirety in Appendix 3.

## Appendix 1

---

### OBJECTIVE

In accordance with the *Federal Information Security Management Act of 2002* (FISMA or the Act), the Office of Inspector General (OIG) performed an independent evaluation to assess the adequacy and effectiveness of the Commission's information security policies, procedures, and practices, and compliance with the requirements of the Act.

### SCOPE

The evaluation was performed between July and September 2006 at the Commission in Washington, DC. Specifically, we performed an evaluation of the Commission's Fiscal Year 2006 unclassified cyber security program. The evaluation included a review of general and application controls in areas such as entity-wide security planning, access controls, application software development, change controls, segregation of duties and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

### METHODOLOGY

To assess the adequacy and effectiveness of the Commission's information security policies and practices, we:

- Reviewed Federal statutes and guidance applicable to ensuring the effectiveness of information security controls over information resources supporting Federal operations and assets such as FISMA guidance and OMB Circular A-130, Appendix III, and NIST standards and guidance;
- Reviewed the Commission's overall cyber security program to evaluate the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA;
- Assessed controls over network operations to determine the ineffectiveness of safeguarding information resources from unauthorized internal and external sources;

- Performed our evaluation in conjunction with our annual audit of the Commission's Financial Statements, utilizing work performed by KPMG LLP (KPMG), the OIG's contract auditor. KPMG's efforts included analysis and testing of general and application controls for systems as well as vulnerability scanning of networks; and,
- Analyzed OIG reports issued between 2003 and 2005 and reviewed other audits and evaluations performed by the Government Accountability Office (GAO) and OMB.

We evaluated the Commission's implementation of the *Government Performance and Results Act of 1993* related to the establishment of performance measures for unclassified cyber security. We did not rely solely on computer-processed data to satisfy our objectives. However, computer assisted audit tools were used to perform probes of various networks and devices. We validated the results of the scans by confirming the weaknesses disclosed with Commission officials and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests.

The evaluation 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 our objective. Accordingly, we assessed internal controls regarding the development and implementation of automated 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 evaluation.

An exit conference was held with Commission officials on September 20, 2006.

### RELATED AUDIT REPORTS

- *Information Security: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements* (GAO 06-527T, March, 2006). GAO reported that in its Fiscal Year (FY) 2005 report to Congress, Office of Management and Budget noted that the Federal Government had made progress in meeting key performance measures for information security; however, uneven implementation of security efforts has left weaknesses in several areas. The FY 2005 reports submitted by the agencies presented a mixed picture of *Federal Information Security Management Act of 2002* (FISMA or the Act) implementation in the Federal Government. In their FY 2005 reports, 24 major Federal agencies generally reported an increasing number of systems meeting key information security performance measures, such as percentage of systems certified and accredited and percentage of contingency plans tested. Nevertheless, progress was uneven. For example, the percentage of agency systems reviewed declined from 96 percent in 2004 to 84 percent in 2005. GAO further reported that Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses.
- *Evaluation Report: The Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2005* (DOE/IG-0704, October 2005). While the Federal Energy Regulatory Commission (Commission) continues to make strides toward improving its unclassified cyber security program, our current evaluation revealed several problems that have the potential to put the Commission's systems at risk. These problems were found in the areas of access controls, configuration management, and corrective action reviews. These problems existed because the Commission had not consistently performed compliance evaluations required by Federal and organization-specific security directives. As a result, the Commission's systems were at risk of disruption of operations, modification or destruction of sensitive data or programs, or theft or improper disclosure of confidential business information.
- *Evaluation of the Federal Energy Regulatory Commission's Cyber Security Program 2004* (OAS-L-04-21, September 2004). Despite making improvements in its unclassified cyber security program, the Commission had not completed contingency planning, risk management, and certification and accreditation of systems. Although the Commission used the National Institute of Standards and Technology (NIST) risk assessment methodology as required by FISMA, it had yet to finalize a risk assessment methodology tailored to its needs - a key step in determining current security vulnerabilities within an organization and implementing mitigating controls. Additionally, at the time of the evaluation the Commission had only completely tested one of its five system-level contingency plans. Successful completion of these ongoing initiatives should help correct remaining cyber security problems at the Commission.

## Appendix 2 (continued)

---

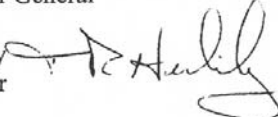
- *Evaluation of the Federal Energy Regulatory Commission's Cyber Security Program 2003* (OAS-L-03-21, September 2003). The evaluation of the Commission's unclassified cyber security program reported that significant progress was made in resolving weaknesses reported during the 2002 evaluation. However, plans for maintaining or resuming critical operations in the event of an emergency or disaster had not been completed.

FEDERAL ENERGY REGULATORY COMMISSION  
WASHINGTON, D.C. 20426

SEP 20 2006

Office of the  
Executive Director

MEMORANDUM TO: Rickey R. Hass  
Assistant Inspector General  
for Financial, Technology, and Corporate Audits  
Office of Inspector General

FROM : Thomas R. Herlihy   
Executive Director

SUBJECT : Management Comments on DOEIG Draft Evaluation Report titled  
"The Federal Energy Regulatory Commission's Unclassified  
Cyber Security Program - 2006"

We appreciate the opportunity to respond to the subject draft report. As you have noted, the security program of the Federal Energy Regulatory Commission (FERC) continues to improve, and achieved a rating of "excellent" for the overall quality of our Certification and Accreditation process. Based on the results of this evaluation, the FERC has an effective security program that meets the requirements of FISMA. We are committed to safeguarding our IT infrastructure and to maintaining a robust cyber security program. Our specific responses to your audit are included below. If you require further assistance please contact Matt Sweet at (202) 502-8926.

**Recommendation 1:** Ensure that existing requirements are implemented for securely configuring the Commission's systems by (a) prohibiting the use of easily guessed, blank, or default passwords that do not adhere to NIST guidelines and (b) correcting systems with improperly configured security settings for various network services.

Concur. FERC has confirmed that there were 6 unique user accounts with blank passwords and 3 user accounts with weak passwords. All of the accounts identified as having blank or weak passwords, were local accounts without network access, and only 2 of all of these local accounts provided any elevated privileges to the computer. There were no accounts that were repeat occurrences from last year. FERC employs Microsoft® Active Directory for user identification and authentication. Active Directory is used to enforce the FERC password complexity policy for all network accounts. FERC agrees that even a small number of accounts whose passwords are not compliant with organizational policy, represents a security issue.

However, in order to exploit any of these local accounts, a perpetrator must have either authorized access to the internal FERC network protected by Active Directory or physical access which would require the circumvention of 3 increasingly restrictive physical layers of defense, using an authorized badge. The only way a person without foreknowledge could have discovered the existence of these particular local accounts would be to scan the network. Any internal scanning process to discover these passwords would have been detected by the FERC Intrusion Detection System (IDS).



Each year FERC has improved its compliance by reducing the number of blank or weak passwords. FERC's goal is to eliminate all non compliant passwords but realizes that as long as personnel have authorized administrative permissions and in the absence of automated checks, some non compliance may occur. Based upon the low number of non compliant local account passwords which represents only 0.23% of the entire user account population, FERC contends that there is only a remote probability that these accounts could be exploited. In addition, any exploitation would result in only limited localized damage, the potential impact is considered negligible. The remote probability and negligible impact support the conclusion that this observation represents a Low<sup>1</sup> risk to FERC.

All of the blank and weak passwords were corrected. Current procedures have been reviewed and found to be adequate to address this low risk. No further action is anticipated.

**Recommendation 2:** Review and update the procedures relating to unused network accounts to enforce the identification and removal of inactive accounts in a timely manner.

Concur. All accounts were reviewed and disabled as appropriate. Standard operating procedures were reviewed and modified to ensure disabling occurs when required. Periodic reviews have been established to assure the process is enforced.

**Recommendation 3:** Ensure that the annual security review processes, used to support the certification and accreditation of systems, thoroughly address the critical control requirements defined by NIST.

Concur. FERC believes it has complied with the guidance in NIST SP 800-26 for annual security reviews. However, FERC acknowledges that its administrative documentation did not appear to satisfy the IG's definition of acceptable artifacts.

FERC has chosen systems certification and annual security review processes that balances risk and cost. When appropriate, the methodology employed leverages security assessment activities already performed during the course of the fiscal year, to allow for a timely assessment of the effectiveness of the system's management, operational, and technical controls.

FERC has an effective change management process that allows us to closely monitor our systems and to document all changes. Given this level of oversight, FERC is able to determine the appropriate level of updates necessary for our security documentation for systems recertification in a cost-effective manner. Utilizing our enterprise quarterly scans, periodic system scans, configuration change notice processes, security test and evaluation processes, and annual contingency testing, we are able to get a comprehensive view of our systems security posture. Therefore, the FERC is convinced that we have followed our C&A Methodology in order to meet the goals of protecting our information systems and to carry out the mission of the FERC.

---

<sup>1</sup> FERC's C&A Methodology: Injury accrues to the organization and its parent organizations' interests if the information is compromised; would cause only minor financial loss or require only administrative action for correction.

## Appendix 3 (continued)

---

In accordance with federal mandates, FERC is also required to perform annual reviews of its security controls for all of its major applications and general support systems. In order to fulfill the OMB mandate and remain consistent with our methodology, one part of our annual review process is either a full certification when due or a recertification when scheduled. For the FERC, recertification requires, at a minimum, interviews with key stakeholders in order to determine current system security status, review of the progress of resolutions for any outstanding weaknesses identified in the corrective action plan, performance and analysis of system vulnerability scans, and review of results with system owners. Annual reviews also incorporate quarterly enterprise scans, contingency testing, and security test and evaluation for technical controls.

In response to the current recommendation from the IG, FERC has completed the administrative updates to the NIST SP 800-26 compliant self-assessment questionnaires for all of its major applications and general support system within the 2006 fiscal year.

**Comment on Appendix 2:** FERC understands that the inclusion of reference to GAO 06-52T, March 2006, in Appendix 2 of this year's IG audit report reflects the IG's concern regarding the general development of security programs and security awareness government wide. We believe we are addressing those concerns as evidenced by the continuous improvement we have made to our cyber security program and the 98% success rate of our Security Awareness Training.

## 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 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 Judy Garland-Smith (202) 586-7828.

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.energy.gov/>

Your comments would be appreciated and can be provided on the Customer Response Form