

DOE/IG-0568

AUDIT
REPORT

REMOTE ACCESS TO UNCLASSIFIED
INFORMATION SYSTEMS



SEPTEMBER 2002

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



U. S. DEPARTMENT OF ENERGY
Washington, DC 20585

September 13, 2002

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Audit Report on "Remote Access to Unclassified Information Systems"

BACKGROUND

Like most private sector and government organizations, the Department of Energy has an aggressive program to provide its Federal and contractor personnel with the ability to remotely access a number of unclassified information systems. Such access allows travelers, telecommuters and those who occasionally work off-site to more easily perform business-related functions from remote locations. Personnel are able, for example, to retrieve electronic mail, access business or other operational systems and administer systems or networks by using government or privately-owned computer equipment. Generally, remote access to the Department's networks is achieved through dial-in modems or through internet connections.

While the benefits of such access are clear, there is a corresponding increase in certain inherent risks, most importantly, the potential for unauthorized access to the Department's information systems. Based on several recent investigative cases relating to attempts to intrude into the Department's systems, we initiated this audit designed to assess the Department's performance in managing the risk associated with remote access to unclassified information systems.

RESULTS OF AUDIT

The majority of the offices we reviewed had not adequately protected information systems from unauthorized remote access. Although we found several offices which had implemented effective risk-mitigation strategies, of the 13 organizations included in our review:

- Ten had not considered the risk associated with remote access when developing cyber security protection plans;
- Nine had not developed specific guidance addressing remote access security requirements; and,
- Nine had not required the use of protective measures such as personal firewalls, and up-to-date virus protection and systems software when accessing network resources.

Inadequate protective measures over remote access placed the Department's critical unclassified information systems at risk of data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive or Privacy Act information. We

concluded that the Department needs to better enforce requirements for risk assessments, provide additional guidance for security implementation and evaluation, and establish performance measures related to remote access risk mitigation. The report includes recommendations to implement these actions.

In our *Special Report on Management Challenges at the Department of Energy*, (DOE/IG-0538, December 2001), we concluded that security of cyber assets is one of the most significant challenges facing the Department. Systematic development and implementation of computer security is essential to mitigating the risk of compromise to the Department's critical information technology resources.

Specific information regarding programs and sites reviewed has been omitted from this report because of security concerns. Cognizant officials were provided information on specific vulnerabilities identified during our audit fieldwork.

MANAGEMENT REACTION

Management agreed with our recommendations and indicated that certain corrective actions were in process or had been completed. In response to our report, management pledged to implement a new security directive, implementing guidance and to improve security planning. Also, management stated that direction had been given to specifically address remote access security during the self-assessment process.

Attachment

cc: Chief of Staff

Under Secretary for Energy, Science and Environment
Acting Administrator, National Nuclear Security Administration
Assistant Secretary for Environmental Management
Assistant Secretary for Fossil Energy
Director, Office of Science
Director, Office of Security
Director, Office of Management, Budget and Evaluation/Chief Financial Officer
Administrator, Energy Information Administration
Chief Information Officer

REMOTE ACCESS TO UNCLASSIFIED INFORMATION SYSTEMS

TABLE OF CONTENTS

Overview

Introduction and Objective.....	1
Conclusions and Observations	1

Remote Access Related Performance Issues

Details of Finding.....	3
Recommendations and Comments	6

Appendices

Scope and Methodology.....	8
Prior Reports	9
Management Comments.....	11

Overview

INTRODUCTION AND OBJECTIVE

In today's environment, rapid advances in information technology are credited with generating tremendous benefits as well as creating significant and unprecedented risk to government operations. As a result, computer security has become a critical element at all levels of government.

To facilitate business operations, the Department of Energy (Department) and its contractors provide employees the ability to remotely access a number of unclassified information systems. Such access offers travelers, telecommuters, and those who occasionally work off-site or at home the convenience and ability to perform business-related functions from a remote location. Personnel are able to retrieve electronic mail, access business or other operational systems, or administer systems or networks by using government or privately-owned computing equipment. Remote access to the Department's networks is achieved through various methods such as dial-in modems, commercial high-speed Internet services, and other Internet procedures.

As more organizations permit remote access to their networks, complexities associated with protecting information systems increase exponentially. Because the Department's unclassified network is logically connected to a common wide area network and linked to Headquarters and virtually all organizations in the complex, the potential for harm from a single system compromise is significant.

We initiated this audit to assess the Department's performance in managing the risk associated with remote access of unclassified information systems.

CONCLUSIONS AND OBSERVATIONS

While certain organizations had implemented protective measures, the Department's performance in mitigating the risk associated with remote access to unclassified information systems was not adequate. Programs or sites we reviewed had not (1) considered the risk associated with remote access when preparing security plans, (2) developed specific guidance for remote access security, and (3) required protective measures such as personal firewalls and virus protection software.

Federal and Departmental directives require organizations to continually assess the risk to computer systems and maintain security commensurate with that risk. Despite these requirements, vulnerabilities existed because Departmental organizations had not focused sufficient attention on the risk of harm associated with remote

access. Inadequate protective measures placed the Department's critical unclassified information systems at risk of attack from internal and external sources and could ultimately result in data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive or Privacy Act information. Adequate protection against these adverse consequences is important to meeting the President's management agenda initiative regarding the use of information technology to improve government operations.

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

(Signed)
Office of Inspector General

Remote Access Related Performance Issues

Planning and Protective Measures

We reviewed the remote access security strategies of 13 program office or site organizations. Although certain of these organizations had implemented protective measures, many had not developed and implemented strategies sufficient to mitigate the risk associated with remote access to their unclassified information systems. While most organizations had developed security plans and cyber security guidance, related documentation often did not specifically address risks or requirements associated with remote access. Where implemented, protective measures for remote access varied widely in scope and effectiveness.

Security Planning and Implementation Guidance

Most organizations did not perform or had not documented a risk-based approach to identifying remote access threats or specifying protective measures. Of the 13 organizations reviewed, only 4 provided a documented assessment of risk and only 3 of those assessments addressed remote access. In particular, we noted that one organization providing centrally managed network and remote access services to a number of program offices had not performed a risk assessment or specified protective measures even though participating organizations relied on it for security administration.

Consistent with the lack of risk assessments, many of the organizations we reviewed had also not developed specific guidance addressing remote access security requirements. Of the sites or program offices reviewed, we noted that only 4 of 13 had developed guidance that specifically addressed protective requirements for remote access. In contrast, most organizations had developed and implemented extensive security procedures governing access to information systems through internal resources.

Protective Measures

While most organizations required at least some level of protection on Department-owned computers, requirements for remote access using privately-owned equipment was less stringent or non-existent. Of the 13 organizations we reviewed, only 4 had implemented protective measures that were substantially consistent with Federal standards.

Specifically, many users were not required to use protective measures such as personal firewalls, virus protection software, and up-to-date systems software when accessing network resources. While most organizations required installation of anti-virus software, only two required virus definitions to be current prior to connecting remotely. Other than cyber security refresher training, organizations generally did not provide security awareness training related to remote access. The use of hardware-based protections such as one-time password generators, a protective measure that minimizes the risk of additional damage should other measures be compromised, were required by only two of the organizations we visited. Without such measures, each remote connection or session exposed the Department's networks to attack by malicious users.

In contrast, one program office we reviewed had well-developed remote access security procedures. This office independently managed its network service and aggressively enforced protective requirements. Remote users were required to attend remote security awareness training and sign a user accountability form prior to being granted access. Users were provided with security features without regard to whether the remote machines were Department or privately-owned. Prior to permitting network access, automated techniques were used to access the remote equipment and verify that the necessary security features had been correctly installed. This organization regarded remote access as a privilege and terminated the service of users who did not maintain adequate protective measures.

Requirements for Risk Based Security and Remote Access Protection

Federal and Departmental directives require organizations to continually assess the risk to computer systems and maintain security commensurate with that risk and consistent with standards. For instance, the Government Information Security Reform Act of 2000 and Office of Management and Budget (OMB) Circular A-130 require agencies to adopt a risk-based, life cycle approach to improving computer security. Specifically, agency security planning should establish acceptable levels of risk and rules covering such matters as work at home, individual accountability, awareness training, dial-in access, connection to the Internet, unofficial use of equipment, assignment and limitation of system privileges; and periodically reviewing security controls for adequacy. In addition, Departmental directives, such as Department Notice 205.1 "*Unclassified Computer Security Program*," require each organization to specify information resources to be protected and protective mechanisms to be used to ensure that all unclassified information resources under its purview are protected in a manner that is consistent with threats to it and its missions at all times.

The Department's cyber security architecture also requires that remote access implementations impose security provisions consistent with those imposed upon other on-site users. This guidance echoes the recommendation by the Federal Computer Incident Response Center that each remote user's system be afforded a minimum level of protection consistent with that of the parent network, such as installing and validating anti-virus software and updating operating system security patches prior to allowing remote connection. The National Institute of Standards and Technology (NIST) also recommended that a personal firewall be used at all times on computers used for remote access.

Attention to Remote Access Security

Departmental organizations had not focused sufficient attention on the risk of harm associated with remote access to unclassified information systems. Although the Department had developed guidance addressing remote access, many of the organizations focused the majority of their protective measures on preventing Internet-based intrusions. The insufficient focus of most organizations on remote access is demonstrated, in part, by the fact that few organizations monitored access activity or maintained detailed information such as type and owner of equipment or levels and types of access granted. Most sites also did not evaluate remote access security when performing periodic oversight or self-assessment activities. Consistent with the overall lack of focus in this area, organizations also had not developed specific performance measures or metrics to measure progress. Where cyber security related site or organization-level goals had been established, most were non-specific and focused only on overall improvements in the cyber security area. Because of the lack of attention, organizations did not devote the resources necessary to assessing the risk associated with remote access.

Unclassified Information Systems

Inadequate protective measures placed the Department's critical unclassified information systems at risk of attack from internal and external sources and could ultimately result in data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive or Privacy Act information. In a recent report to management, the Office of Inspector General disclosed that a malicious user was able to gain access to an employee's government-owned laptop. This occurred while the employee was remotely connected to the site's network while simultaneously connected to his personal Internet Service Provider (ISP) at his residence. The review identified inadequate remote access controls and configuration management requirements at the site that may have contributed to the compromise of the laptop. In addition to directly endangering Departmental networks,

hackers gaining control of employees' computers could later monitor remote access sessions and capture passwords or other sensitive data. Without adequate attention to remote access security, the Department's networks and information systems will continue to be subject to a significant risk of compromise. As we have previously reported, the failure to ensure the security and confidentiality of personal information could subject employees to the risk of identity theft and intelligence targeting and the Department to potential litigation.

RECOMMENDATIONS

To correct the specific vulnerabilities noted in this report, we recommended that, for the sites and offices within their responsibility, the Administrator, National Nuclear Security Administration; the Assistant Secretaries for the Office of Environmental Management and Office of Fossil Energy; and the Director, Office of Science:

1. Require sites which have not assessed risk or developed and implemented protective measures to do so immediately; and,
2. Require sites or offices to issue clear guidance for remote access services consistent with Federal, Departmental, and the NIST requirements for remote access security.

To enhance overall security for remote access to unclassified information systems, we recommend that the Director, Office of Security work with the Chief Information Officer to:

3. Reemphasize the requirement for organizations to perform formal risk assessments and to develop and implement protective measures commensurate with the assessed level of risk;
4. Require that remote access security be specifically evaluated during the security self-assessments required by the Government Information Security Act of 2000; and,
5. Establish specific, quantifiable performance measures for improving remote access services controls and include them in the Department's Cyber Security Metrics program and the organization's Annual Performance Plan.

MANAGEMENT REACTION

The Administrator, National Nuclear Security Administration; Assistant Secretaries for the Office of Environmental Management and Office of Fossil Energy; and the Director, Office of Science, Director, Office of Security; and Chief Information Officer concurred with our recommendations. Management indicated that certain corrective actions were in process or had been completed. Management specifically pledged to develop new security policy, associated implementing guidance, and to improve security planning. Program level management pointed out that Departmental policy direction was required to effectively address remote access issues raised in the report. Also, management stated that direction had been given to specifically address remote access security during the self assessment-process. Finally, management noted that although performance measures are the responsibility of each program office, the requirement for such measures will be established in new Departmental directive and guidance. Management's comments are attached as Appendix 3.

AUDITOR COMMENTS

We consider management's comments and actions responsive to our recommendations and the issues addressed in our report.

Appendix 1

SCOPE

The audit was performed between December 2001 and May 2002. We assessed the Department's performance in managing the risk associated with remote access of unclassified information systems. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To accomplish our objectives, we:

- Reviewed Federal Regulations such as the Government Information Security Reform Act, Government Performance and Results Act, OMB Circular A-130, Departmental Directives and guidance pertaining to information system security;
- Reviewed relevant reports issued by the Office of Inspector General, the General Accounting Office, and Office of Independent Oversight and Performance Assurance;
- Held discussions with officials and staff at various organizations; and,
- Assessed organizational security practices and analyzed remote access user details.

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.

PRIOR REPORTS

- *Management Challenges at the Department of Energy*, (DOE/IG-0538, December 2001). Among other things, the report identified information technology, performance management, and security and safety as the most serious management and performance challenges the Department faces. Consistent with the requirements of the Government Performance and Results Act, the Department should aggressively work to develop and implement performance goals and measures that directly address each of the management challenges identified in this report. Further, actual performance should be assessed against these goals and measures and be independently validated.
- *Inspection of Cyber Security Standards for Sensitive Personal Information* (DOE/IG-0531, November 2001). The report concluded that the Department does not always meet the requirements of the Privacy Act of 1974, the Freedom of Information Act (FOIA), or the Computer Security Act of 1987 because the Department: (1) does not have a Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; (2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and (3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.
- *The Department's Unclassified Cyber Security Program* (DOE/IG-0519, August 2001). The report determined that while the Department has made improvements in its unclassified cyber security program, the program did not adequately protect data and information systems as required by the Government Information Security Reform Act. Problems with design and implementation of cyber security policy, including a lack of monitoring and specific, focused performance measures, contributed to these weaknesses and adversely affected the effectiveness of the entity-wide program. Observed weaknesses increased the risk that critical systems, a number of which enable delivery of essential services to members of the public and other Federal agencies, could be compromised or disabled by malicious or unauthorized users.
- *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996*, (DOE/IG-0507, June 2001). The report summarized 13 information technology (IT) related Office of Inspector General reports. Cumulatively, these reports demonstrated systemic problems with the Department's approach to IT management and its method of addressing requirements of the Clinger-Cohen Act of 1996 (Act). Specifically, the Department had not satisfied major requirements of the Act to develop and implement an integrated, enterprise-wide, IT architecture, closely monitor policy implementation efforts, and acquire IT related assets in an effective and efficient manner. We attributed the problems identified, in part, to the Department's decentralized approach to information technology management and oversight and the organizational placement of the Chief Information Officer (CIO). The Department has recently taken a number of actions designed to improve the overall management of information technology resources, including making the CIO a direct report of the Secretary.

Appendix 2 (continued)

- *Virus Protection Strategies and Cyber Security Incident Reporting*, (DOE/IG-0500, April 2001). The Department's virus protection strategies and cyber security incident reporting methods did not adequately protect systems from damage by viruses and did not provide sufficient information needed to manage its network intrusion threat. These problems existed because the Department had not developed and implemented an effective enterprise-wide strategy for virus protection and cyber security incident reporting.
- *Department of Energy's Consolidated Financial Statements*, (DOE/IG-FS-01-01, February 2001). The report identified three reportable weaknesses in the Department's system of internal controls pertaining to performance measures, financial management, and unclassified information system security. Specifically, performance goals, in many cases, were not output or outcome oriented and/or were not meaningful, relevant, or stated in objective or quantifiable terms. The Department also had certain network vulnerabilities and general access control weaknesses.
- *Internet Privacy*, (DOE/IG-0493, February 2001). The Department's method of collecting data from users of its publicly accessible web sites was not always consistent with Federal regulations. Specifically, some web sites were collecting data by unapproved or undisclosed means and a number of web sites did not display conspicuously located, clearly written privacy notices.
- *Unclassified Computer Network Security at Selected Field Sites*, (DOE/IG-0459, February 2000). Departmental sites audited had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. Each site evaluated had network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, outdated software with known security problems, and/or problems with firewall configuration.
- *Review of the U.S. Department of Energy's Information Management Systems*, (DOE/IG-0423, August 1998). The report stated that the CIO lacked the authority and resources necessary to ensure development of information architectures at the program office level, which form the building blocks of a Departmental architecture. The report added that, as a result, the Department had not developed and implemented information technology architecture, although its Strategic Plan called for the implementation of Department-wide information architecture with supporting standards by January 1998.



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

JUN 24 2002

MEMORANDUM FOR Frederick D. Doggett
Deputy Assistant Inspector General
for Audit Services

FROM: Anthony R. Lane *Anthony R. Lane*
Associate Administrator for
Management and Administration

SUBJECT: Comments to IG Draft Report, "Remote Access to
Unclassified Information Systems"

The National Nuclear Security Administration reviewed the Inspector General's draft report "Remote Access to Unclassified Information Systems." The Administration agrees with the recommendations that are directed towards NNSA. Both the NNSA's Cyber Security Program Manager and the NNSA's Chief Information Officer have initiatives underway that will address, in part, the Inspector General's concerns. NNSA will coordinate our actions with appropriate departmental offices where necessary.



Printed with soy ink on recycled paper



Department of Energy
Washington, DC 20585

AUG 7 2002

MEMORANDUM FOR FREDERICK D. DOGGETT
DEPUTY ASSISTANT INSPECTOR GENERAL
FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM

KAREN S. EVANS 
CHIEF INFORMATION OFFICER

SUBJECT:

Draft Report on "Remote Access to Unclassified Information Systems"

The Office of the Chief Information Officer (CIO) and the Office of Security concur with your recommendations and our response is attached. In addition, we have received, and concur with, the attached responses from the Office of Science and Office of Fossil Energy. The Office of Environmental Management (EM) has also provided a response to the Office of CIO. The EM response is currently under review by this office and we will comment under separate cover. The National Nuclear Security Agency will respond directly to the Office of Inspector General.

If you have further questions please contact Ms. Carol Bales, Deputy Associate CIO for Cyber Security, on 202-586-7865

Attachments:

Office of Security Memorandum
Office of Science Memorandum
Office of Fossil Energy Memorandum



Printed with soy ink on recycled paper

Appendix 3 (continued)



Department of Energy

Washington, DC 20585

July 12, 2002

MEMORANDUM FOR KAREN S. EVANS
CHIEF INFORMATION OFFICER

FROM: RAYMOND L. JOBBACH
DIRECTOR
OFFICE OF SCIENCE

SUBJECT: Comments on IG Draft Report, "Remote Access to
Unclassified Information Systems"

The Office of Science (SC) has reviewed the IG Draft Report, "Remote Access to Unclassified Information Systems." SC agrees with the recommendations in the draft report.

The report does not specifically identify the DOE Headquarters organizations that were found to be at risk; however, SC Headquarters computer support cyber security efforts continue on an on-going basis. Efforts include assessing all known security risks and taking appropriate measures to prevent unauthorized access and/or compromise to SC unclassified information by remote access users, specifically in the referenced areas of cyber security planning, remote access security guidance, and personal firewall/virus protection for offsite workstations.

Additional comments are attached.

Attachment

cc:
George Dudley, IM-1



Printed with soy ink on recycled paper

Appendix 3 (continued)

MEMORANDUM

TO: JOHN L. PRZYSUCHA, ASSOCIATE CHIEF INFORMATION OFFICER,
OFFICE OF INFORMATION TECHNOLOGY REFORM

FROM: ROBERT C. PORTER, DIRECTOR, OFFICE OF COMMUNICATIONS,
OFFICE OF FOSSIL ENERGY

SUBJECT: REVIEW AND CONCURRENCE ON RECOMMENDATIONS FROM IG
REPORT, A02AT007, ENTITLED "REMOTE ACCESS TO UNCLASSIFIED
INFORMATION SYSTEMS"

The Office of Fossil Energy (FE) concurs with the recommendations cited in the subject audit report. Additionally, FE has taken proactive steps to include procedures addressing the objectives of recommendations 1 and 2 in its Computer Security Program Plan. Moreover, FE is currently reviewing and will provide comments on the Department's draft Remote Access Policy prepared by the Office of the Chief Financial Officer.

Should you have any questions or concerns, please feel free to contact, Kevin Clark, (202) 586-2667.

DOE F 13259
(8-89)
EPO (07-90)

United States Government

Department of Energy

memorandum

DATE: AUG 26 2002

REPLY TO
ATTN OF: EM-7.2

SUBJECT: Draft IG Report on Remote Access to Unclassified Information Systems

TO: Frederick D. Doggett, IG-32

The Office of Environmental Management (EM) has reviewed the subject report and concurs with the findings and recommendations. EM notes, however, that there are issues raised by the report involving remote access practices that require DOE policy direction to ensure effective implementation. These issues include the legal ramifications of installing government-mandated software on privately owned computers and the liability issues involving security breaches in such environments. EM strongly urges that the IG coordinate with, and seek the approval of, the General Counsel prior to issuing recommendations that may conflict with legal precedent or statutory restrictions on cyber security matters.

EM responds to the specific IG recommendations as follows:

Recommendation 1:

Requires sites which have not assessed risk or developed and implemented protective measures to do so immediately.

EM Response:

All EM sites have already taken measures to implement and deploy cyber security counter-measures as a management best practice, apart from any formal risk assessment that may or may not have been executed. EM fully concurs that the configuration of these systems should be driven in part by risk assessment conclusions. EM will promulgate a preferred methodology across the enterprise that itemizes risk factors that must be taken into consideration when evaluating mission information protection schemas for remote access. These risk factors will be regularly updated to take into account changes in the nature and composition of threats against our information assets and the systems that support them. EM plans to distribute a formal risk assessment methodology for review within 90 days of the date of this response.

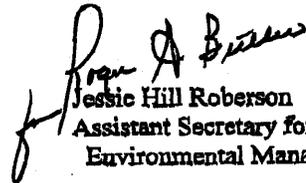
Recommendation 2:

Require sites or offices to issue clear guidance for remote access services, consistent with Federal and Departmental guidance, that substantially complies with remote access security guidance issued by the National Institute of Standards and Technology.

EM Response:

NIST 800-46, Security for Telecommuting and Broadband Communications, which is presently undergoing comment revision, is the guidance document that will drive remote access practices for conventional remote access technologies within EM. Environmental Management will issue clear guidance when the relevant NIST document is officially released out of Draft. EM Headquarters is designing an advanced remote access architecture that fully meets NIST FIPS and is a key component to support flexiplace across the EM complex. EM expects to implement the proof-of-concept design in the December 2002 time frame.

If you wish to discuss these responses or need additional information, please contact Daniel Pitton of my staff at (202) 586-7228.


Jessie Hill Roberson
Assistant Secretary for
Environmental Management

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.