DOE/IG-0500

AUDIT REPORT

VIRUS PROTECTION STRATEGIES AND CYBER SECURITY INCIDENT REPORTING

APRIL 2001

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

April 5, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Audit Report on "Virus Protection Strategies and Cyber Security Incident Reporting"

BACKGROUND

Information Technology (IT) plays an integral role in the programs and operations of the Department of Energy. In Fiscal Year 2001, the Department budgeted $1.4 billion for the acquisition and maintenance of IT related resources, a portion of which supports the Advanced Strategic Computing Initiative. These resources, and the programs they support, are vulnerable to malicious software, viruses, trojans, worms (collectively referred to as viruses), and cyber security attacks. To effectively protect its IT resources, the Department must ensure that its virus protection and detection capabilities as well as its cyber security incident reporting practices are "state of the art."

The objective of this audit was to determine whether the Department's virus protection strategies and cyber security incident reporting methods protect systems from damage by malicious software and provide information needed to manage network intrusion threats.

RESULTS OF AUDIT

The Department's systems were not adequately protected from damage by viruses because of shortcomings in its virus protection strategies and cyber security incident reporting methods. Further, the incident reporting scheme in use at the time of our audit did not provide sufficient information to appropriately manage the Department's network intrusion threat. Specifically, we found that:

- site virus protection strategies were not consistent with best practices and varied widely on a site-by-site basis in levels of coverage and effectiveness; and,

- the Department was unable to accumulate sufficient information necessary to manage its network intrusion threat and risked compromising evidence of computer crimes because of problems with reporting cyber security incidents to monitoring officials.

MANAGEMENT REACTION

We made a number of recommendations designed to improve the effectiveness of the Department's virus protection strategy and cyber security incident reporting programs. Management agreed, in general, with the recommendations and agreed to develop policy and establish specific performance goals to measure the success of policy implementation. Management agreed, as well, to continue to investigate whether a centrally managed procurement for virus protection software is viable or if alternatives exist and stated a decision will be made in 90 days.

By design, the recommendations included in this report are policy-oriented and are, therefore, directed to Department IT and Security policymakers. Based on our discussions with responsible officials, it appears unlikely that policy changes alone, as meaningful as they may be, will result in improving the Department's performance in the areas covered by this report. Given the decentralized organizational structure of the Department of Energy, success is dependent upon a cooperative effort that includes the active participation of those responsible for making policy as well as Headquarters and local program officials–both Department and NNSA. To this end, we believe that program officials should play a significant role in developing the policies that they will ultimately have to implement to improve the Department's virus protection and cyber security reporting programs.

Attachment

cc: Administrator, National Nuclear Security Administration
Acting Director, Office of Security and Emergency Operations
Acting Chief Information Officer

VIRUS PROTECTION STRATEGIES AND CYBER SECURITY INCIDENT REPORTING

TABLE OF CONTENTS

Overview

Virus Protection and Incident Reporting

Appendices

OVERVIEW

INTRODUCTION AND OBJECTIVE

The Department of Energy (Department) devotes a significant amount of its annual budget to the acquisition and maintenance of information technology (IT) related resources. In Fiscal Year (FY) 2001, the Department budgeted $1.4 billion for IT investments, a portion of which supports weapons programs such as the Advanced Strategic Computing Initiative. Protecting these resources from malicious software, viruses, trojans, worms (collectively referred to as viruses), and potential attacks is of paramount concern. The Office of Chief Information Officer (CIO) and the Department's Computer Incident Analysis & Assistance Center (CIAC) have key roles in helping the Department provide an effective information security infrastructure. The CIO is charged with promulgating cyber security policy and ensuring its implementation, while CIAC is charged with collecting, analyzing, and disseminating data on cyber security incidents throughout the Department.

In recent years, the computing and information management environment within the Department has changed tremendously. The occurrences of viruses and attempted network intrusions throughout the Department have increased dramatically. To be proactive in protecting its IT resources, the Department must develop a complete picture of the type of cyber security incidents occurring throughout the complex. The entire Department must endeavor to continually improve its virus protection and detection capabilities as well as cyber security incident reporting to wage a successful protection and response campaign. According to the National Institute of Standards and Technology, best practices for virus protection call for a tiered approach that includes clear policies and procedures, the installation of software on all servers, desktops, laptops and Internet gateways, and frequent software updates.

The objective of this audit was to determine whether the Department's virus protection strategies and cyber security incident reporting methods protect systems from damage by malicious software (viruses) and provide information needed to manage its network intrusion threat.

CONCLUSIONS AND OBSERVATIONS

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. For example, site virus protection strategies were not consistent with best practices and varied widely in levels of coverage and effectiveness. Also, the Department was unable to accumulate sufficient information necessary to manage its network intrusion threat and risked compromising evidence of computer crimes because many organizations did not report or provided only limited information regarding cyber security incidents to CIAC. The Clinger-Cohen Act and other Federal regulations required the Department to establish a comprehensive cyber security program that had a robust virus protection strategy and an incident response capability that identified the overall cyber security threat to the complex. These problems existed because the Department had not developed and implemented an effective enterprise-wide strategy for virus protection and cyber security incident reporting. As a result, the Department spent over $3.8 million annually for a computer incident response capability that cannot adequately assess the threat experienced by the complex as a whole. In addition, the Department could improve consistency, increase overall coverage, and save as much as $3 million by adopting an enterprise-wide approach to virus protection software acquisition.

Management should consider the issues discussed in this report when preparing its yearend assurance memorandum on internal controls.

Signed
Office of Inspector General

VIRUS PROTECTION AND INCIDENT REPORTING

Protection and Reporting

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. For example, site virus protection strategies were not consistent with best practices and varied widely in levels of coverage and effectiveness. The Department was unable to accumulate sufficient information necessary to manage its network intrusion threat and risked compromising evidence of computer crimes because many organizations did not report or provided only limited information regarding cyber security incidents to CIAC. Furthermore, the Department's primary control for the development and implementation of site-specific Cyber Security Program Plans (Program Plan) was not working properly.

Virus Protection

Site virus protection strategies were not consistent with best practices and varied widely in levels of coverage. Contrary to best practices, most sites did not use a tiered strategy that included protection of all desktops, laptops, servers, and Internet gateways or firewalls. Currently, Departmental entities are free to choose a virus protection strategy when designing their Program Plan. As such, each site reviewed had developed a customized approach that relied on individually purchasing a combination of virus protection software packages that did not necessarily protect all computers. For instance, Lawrence Livermore National Laboratory relied primarily on desktop software for virus protection and did not have virus software installed on its servers. DOE Headquarters had a tiered strategy that included protection at the e-mail server and desktop computer, but did not consistently protect systems from infected e-mails sent from within Headquarters elements. Lawrence Livermore National Laboratory officials informed us that they began adding additional virus protection software on other key components of their network to strengthen their virus defense during January 2001.

In many of the systems on which virus protection software had been installed, its effectiveness was limited because it was not properly updated. For a protection strategy to be effective, virus definition files must be continually updated because new virus attacks are continually promulgated. These definition files contain attributes that virus protection software uses to recognize the "signature" of known viruses. Departmental elements used a variety of techniques to update virus definition files but were not always successful in reaching all computers. Of the 169 computers we tested at 9 Departmental elements, we noted that virus definition updates varied in age from current (within a week) to about 23 months. For example, the age of definition files at the Sandia National Laboratory in California ranged from 1 to 772 days and those at the Oak Ridge Operations Office's ranged from 5 to 540 days. In addition, we found that laptops were the least protected computers throughout the Department. Of the 15 laptops we tested, 14 or 93 percent, did not have current file definitions. The definitions ranged from 6 days to as old as 540 days, with no protection at all installed on 2 computers. The Nevada Operations Office installation of virus protection software on new laptops contained virus definitions that were over 600 days old. Nevada officials informed us that they are revising their maintenance approach for laptops to automatically update virus definition files.

Incident Reporting

While the Department had developed and implemented an incident response capability, incomplete reporting by sites and program elements severely limited its effectiveness. Based on Departmental statistics, less than 50 percent of sites with reporting responsibility consistently reported cyber security incidents. Of those reporting, only 5 sites reported all significant cyber security incidents to CIAC. While the number of sites that report incidents is increasing, many sites still do not report virus incidents and judgmentally select which other cyber security incidents to report. For example, Oak Ridge and Sandia National Laboratories did not report all virus incidents to CIAC. In addition, most of the sites we visited summarized and selected which incidents (scans, probes, attempted intrusions, intrusions, and viruses) to report. Lawrence Livermore and Oak Ridge National Laboratories had an automated system that reported all incidents except viruses. Without complete data, CIAC is unable to accurately assess the threat to the Department's information systems and to provide complete and up-to-date predictive warnings.

Incomplete and untimely reporting also adversely impacts the Department's ability to satisfy internal and external reporting requirements and to protect evidence in cases with investigative potential. Based on subject matter and severity of the threat, cyber security incidents require specific responses by various organizations within the Department. Without accurate reporting, internal organizations such as the Offices of Security and Emergency Operations, the CIO, and Counterintelligence may not be prepared to initiate timely and appropriate corrective actions or countermeasures. In addition, lack of reporting may jeopardize systems of other Federal organizations since accurate threat data cannot be provided to national-level organizations such as the Federal Computer Incident Response Capability and the National Infrastructure Protection Center. Incomplete reporting also limits the Department's ability to protect or preserve evidence in cyber security incidents. For example, of the 103 successful intrusions reported to CIAC in FY 2000, the Office of Inspector General's Technology Crimes Section reported that it was only able to open investigations in 12 cases because of the lack of notification or timely preservation of evidence.

Cyber Security Program Plans

The Department's primary control for the development and implementation of site-specific Cyber Security Program Plans was not working properly. Each Departmental element was to submit a draft Program Plan to the CIO for review and subsequently submit an approved Program Plan for inclusion in the CIO's central repository. Although Departmental Notice 205.1, "Unclassified Cyber Security Program" (Notice), required the Program Plan to specify the frequency of updating definition files, only six of the ten Program Plans reviewed contained that information. Even though Oakland Operations Office's Program Plan stated definition files would be updated weekly, we found the implementation to be wanting in that 37 of 38 computers judgmentally checked had definition file dates that exceeded their Program Plan guidelines. Generally, the Program Plans neither contained clear definitions of the cyber security incidents to be reported, nor contained comprehensive reporting protocols. Although specifically required, six reporting elements did not submit draft plans to the CIO for review. As of December 2000, only 2 of the 108 elements complied with Departmental requirements to provide an approved plan, incorporating review comments, to the CIO for retention. After completion of our audit field work, the CIO reported 78 additional elements returned approved Program Plans for retention leaving 28 plans outstanding.

Protection and Reporting Requirements

The Clinger-Cohen Act and other Federal regulations required the Department to establish a comprehensive cyber security program that has a robust virus protection strategy and an incident response capability to identify the overall cyber security threat to the complex. A minimal virus protection strategy should be based on a tiered strategy. According to the National Institute of Standards and Technology (NIST) and the Critical Infrastructure Assurance Office, this tiered approach should include:

- Formal written policy and procedures detailing the protection strategy, user and management responsibilities, coverage, software updating, and incident reporting;

- The installation and use of virus software on personal computers (desktops and laptops) capable of scanning disks, attachments to e-mails, files downloaded from the Internet, and documents generated by word processing and spreadsheet programs;

- Use of virus software on servers, at Internet gateways or firewalls, to scan e-mail attachments and other downloaded files; and

- Virus software installed on computers when initially configured and, at a minimum, updated weekly.

Federal policy standards setting bodies emphasize that agencies must be continually vigilant in their virus protection strategies. NIST requires that agencies maintain their virus alert defenses through clear policies and procedures, ongoing awareness and education campaigns, effective communication strategies, and effective technology deployment on all computers. The Government's Critical Infrastructure Assurance Office also stresses that information security measures should include software and electronic tools, such as virus software, installed at various points in the client-server architecture.

According to the Office of Management and Budget, the Federal Computer Incident Response Capability and NIST, a computer security incident response capability (incident response capability) should be thought of as a direct extension of the contingency planning process. An agency's incident response capability should be the central capability for dealing with virtually any computer security problem that occurs. It should provide a means for reporting incidents, disseminating important incident-related information to management and users, and coordinating incident handling. The goal of incident response is to mitigate the potentially serious effects of a computer security-related problem. To achieve this aim, an incident response capability requires the involvement and cooperation of the entire agency in reporting cyber security incidents in a timely manner. Such involvement and cooperation is essential for the accumulation of information necessary to manage the Department's network intrusion threat.

Ineffective Enterprise-Wide Strategy

Problems with virus protection and cyber security incident reporting occurred because the Department had not developed and implemented an effective enterprise-wide protection strategy. Departmental implementing guidance for virus protection strategies did not mandate a minimum-level of protection and did not include provisions for the development of an enterprise-wide virus protection software contract. Guidance for cyber security incident reporting did not clearly establish mandatory reporting guidelines and provided no mechanism for enforcement. The absence of specific performance measures also adversely impacted the Department's protection efforts.

Virus Protection Guidance

Departmental implementing guidance for virus protection strategies did not mandate a minimum-level of protection and did not include provisions for the development of an enterprise-wide virus protection software contract. For example, reporting elements were required to specify a virus protection strategy in the Program Plan, however the Department did not mandate a specific minimum level of virus protection. While the CIO provided sites with recommendations on developing a tiered virus protection strategy, the guidance was not mandatory. Consequently, each site developed a plan with varying degrees of coverage that did not necessarily meet best practices or conform to the CIO recommendations. In addition, Departmental Notice 205.1 did not include provisions for the acquisition of an enterprise-wide virus protection software package to be made available to all Federal and contractor elements.

Incident Reporting Guidance

Guidance for cyber security incident reporting did not clearly establish mandatory reporting guidelines and provided no mechanism for enforcement. For example, the Notice did not clearly define what constituted a reportable cyber security incident and consequently each site interpreted and reported incidents differently. In July 2000, the CIO recognized that cyber security incidents needed to be better defined and announced its intention to develop an Indications, Warning, Analysis and Reporting Capability policy. Until this policy was completed, the CIO instructed all Departmental elements to report, at a minimum, successful compromises, infrastructure disruptions, and attempted intrusions to CIAC. The Director of Cyber Programs, Office of Counterintelligence echoed this point in November 2000 indicating that the development of common computer security incident definitions and response protocols to ensure standardized and coordinated responses across the Department remained a significant concern. Yet, to date the revised policy has not been issued. In addition, the Notice and the draft policy did not contain enforcement mechanisms that required either the CIO or Lead Program Secretarial Offices to ensure that all Departmental elements were properly reporting.

Performance Goals

While the Department had developed high-level performance goals with respect to site-level cyber security reviews, specific virus protection and cyber security incident response related performance goals as required by the Government Performance and Results Act of 1993 (GPRA) had not been developed. GPRA requires Federal agencies to establish clear and measurable performance goals for all critical programs. Without specific goals, the Department lacked a basis to measure and demonstrate its performance in this highly sensitive area.

Benefits Not Achieved

The Department spends over $3.8 million annually for a computer incident response capability that cannot adequately assess the threats facing the Department or provide for complete and up-to-date predictive warnings. As such, incomplete reporting of cyber security incidents increased the risk of damage to the Department's IT infrastructure. In addition, the Department could save as much as $3 million by adopting an enterprise-wide approach to virus protection software acquisition.

The Department had not effectively taken advantage of consolidated buying opportunities such as enterprise-wide contracts when procuring virus protection software. As a consequence, sites and program elements procured software independently at prices ranging from $2 to $35 per copy. As noted in our Audit Report on *Commercial Off-The-Shelf Software Acquisition Framework* (DOE/ IG-0463, March 2000), procurement of enterprise-wide licenses allows a diverse organization, such as the Department of Energy, to maximize its return on IT investment by increasing its buying power and gaining economies of scale. As also noted in this report, sites and program elements maintain at least nine different virus protection software products. While the Department has initiated action to standardize desktop computer software, virus protection software standards have not yet been addressed. Pooling the Department's purchases in this area could substantially decrease expenditures for virus protection software and could reduce the risk of damage to its critical information systems by providing a consistent minimum level of virus protection Departmentwide.

Ongoing Security Efforts

To its credit, CIAC is working with the Office of Inspector General's Technology Crimes Section and reporting of cyber security incidents has become more consistent. Also, the CIO is developing an incident reporting policy and attempting to clearly define reportable cyber security incidents and reporting protocols. Once completed, the policy may provide additional guidance to sites on reporting requirements to allow the Department to make cost-effective, risk-based information security decisions. Further, the CIO entered into an enterprise-wide license for network security scanning software that was made available to all Departmental elements. Moreover, the Office of Counterintelligence has collaborated with CIAC to develop and implement the Operational Analysis Center to share data on information security risks within the Department. Nevertheless, proper virus protection and incident reporting within the Department remained a challenge.

RECOMMENDATIONS

To ensure the Department's virus protection strategies and cyber security incident reporting methods sufficiently protect IT resources we recommend that the Director of the Office of Security and Emergency Operations and the Chief Information Officer:

1. Finish the development and implementation of the Indications, Warning, Analysis and Reporting Capability policy, paying particular attention to ensure that the final policy includes clearly defined cyber security incidents to be reported, required incident data collection and evidence preservation methods, standardized reporting forms and/or other mechanisms, and mandatory reporting to CIAC.

2. Develop and implement a program to monitor cyber security incident reporting to ensure that all Departmental elements are properly reporting, including a negative response when no incidents occur during the reporting period.

3. Consistent with GPRA, establish performance goals to measure the success of the Indications, Warning, Analysis, and Reporting Capability policy implementation.

4. Develop a minimal virus protection strategy including an enterprise-wide virus protection software suite, mandate adherence to the strategy, and require the software's usage by all Departmental elements.

MANAGEMENT REACTION

Management agreed, in general, with the recommendations related to virus protection strategies and cyber security incident reporting within the Department. The proposed actions include finalizing DOE Manual 205.X, Handling Cyber Security Alerts and Advisories, Reporting Computer/Cyber Security Incident (Manual), which will clarify responsibilities and processes for responding to cyber security incidents. In addition, management indicated that performance measures were being developed to better judge the effectiveness of the cyber security program and implementation of the Manual.

However, management did not fully agree with recommendation 4. Management partially concurred because they are trying to determine whether the use of an enterprise-wide license for virus protection software is cost-effective. Management agreed to investigate whether a centrally managed procurement for virus protection software is viable or if alternatives exist and make a decision in 90 days.

AUDITOR COMMENTS

Management's comments and proposed actions are generally responsive to the issues raised in this report. With regard to recommendation 4, an enterprise-wide license has been shown to be a cost-effective method of acquiring virus protection software. As stated in the report, pooling the Department's purchases in this area could substantially decrease expenditures for virus protection software and could reduce the risk of damage to its critical information systems by providing a consistent minimum level of virus protection across the complex. The Department should explore alternative funding approaches, such as combining funding from various programs and the National Nuclear Security Administration, to accomplish this goal.

Appendix 1

SCOPE

The audit was performed between August 2000 and February 2001 at Departmental Headquarters in Washington, DC; the Lawrence Livermore National Laboratory in Livermore, California; the Sandia National Laboratory and Albuquerque Operations Office in Albuquerque, New Mexico; the Nevada Operations Office and Bechtel Nevada in Las Vegas, Nevada; and the Oak Ridge Reservation in Oak Ridge, Tennessee. Based on our on-site work and survey results, we accumulated statistics on 12 separate Departmental entities with regard to virus protection and incident reporting strategies.

METHODOLOGY

To accomplish our objectives, we:

- Reviewed applicable laws and regulations pertaining to the use and acquisition of information technology. We also reviewed reports by the Office of Inspector General, the General Accounting Office, and various task forces and advisory groups.

- Reviewed Departmental strategic plans and performance goals for compliance with the Government Performance and Results Act of 1993.

- Reviewed numerous documents related to the use and acquisition of virus protection software. We also reviewed Departmental planning documents related to cyber security and incident reporting.

- Tested a judgmental sample of Federal and contractor computers for current virus protection software and definition dates.

- Held discussions with program officials and personnel from the Offices of the Chief Information Officer, Procurement and Assistance Management, and CIAC. We also held discussions with various officials and staff at the operations offices and laboratories we visited.

- Reviewed information from the Department of Defense regarding initiatives undertaken to establish an enterprise-wide virus protection software contract. Discussions were also held with information technology vendors to gain their perspective on the Department's acquisition practices.

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 use and acquisition of virus protection software. 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. We did not rely on computer-processed data to accomplish our audit objectives. An exit conference was held with appropriate Headquarters officials on February 26, 2001.

Appendix 2

RELATED OFFICE OF INSPECTOR GENERAL AND GENERAL ACCOUNTING OFFICE REPORTS

This review concerned the Department's efforts to develop a comprehensive virus protection and incident reporting strategy and included a review of the Department's framework for software acquisitions, consisting of software standards and enterprise-wide software contracts. Prior related Office of Inspector General and General Accounting Office reviews include:

- *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 an information technology architecture, although its Strategic Plan called for the implementation of a Departmentwide information architecture with supporting standards by January 1998.

- *Audit of the Department of Energy's Commercial Off-The-Shelf Software (COTS),* DOE/IG-0463, March 2000. The report found that the Department had not developed and implemented software standards or effectively used Departmentwide contracts, key components of a COTS acquisition framework. The Department had not made effective use of enterprise-wide software contracts. Instead the Department allowed various offices to duplicate procurement efforts by separately negotiating and awarding contracts for the same application. It also noted the Department had at least 9 different virus software packages throughout the department.

- *Audit of the Department of Energy's Corporate and Stand-Alone Information Systems,* DOE/IG-0485, September 2000. The report stated that the Department had not fully developed and implemented an application software strategy designed to reduce or eliminate duplicative systems.

- *Audit of the Department of Energy's Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection*, DOE/IG-0483, September 2000. The report stated the Department had not implemented its critical infrastructure protection plan to mitigate significant vulnerabilities, or assure the continuity and viability of its critical infrastructures. Therefore, the Department could not achieve the purpose of PDD 63.

- *"ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements*, GAO/AIMD/00-171, May 2000. The report stated that computer attacking tools and techniques are becoming increasingly sophisticated; viruses are spreading faster as a result of the increasing connectivity of today's networks, there is no "silver bullet" solution such as firewalls or encryptions. ILOVEYOU once again proved that Governmentwide reporting mechanisms are ineffective.

- *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000*, GAO/AIMD/00-229, June 2000. The report stated that the federal government itself must be a model of good information security. Significant computer security weaknesses ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, to nonexistent or weak continuity of service plans pervade virtually every major agency.

- *Vulnerabilities in DOE's System for Unclassified Civilian Research*, GAO/AIMD/00-140, June 2000. The report stated that the Department's unclassified information systems for scientific research are not consistently protected at all Department laboratories. The report also stated that while the Department has reported significant improvements, not all Departmental facilities have been reporting incidents to the Department's CIAC, and incidents are not consistently reported.

- *Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD/00-295, September 2000. The report stated evaluations of computer security published since July 1999 continue to show that federal computer security is fraught with weaknesses and that as a result, critical operations and assets continue to be at risk.

IG Report No.: DOE/IG-0500

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 alternative 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.