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

Audit Report

Certification and Accreditation of Unclassified Information Systems

DOE/IG-0752

January 2007

Department of Energy

Washington, DC 20585

January 3, 2007

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Certification and Accreditation of Unclassified Information Systems"

BACKGROUND

Information systems are essential to accomplishing the Department of Energy's environmental, energy, and national security-related missions. Actions to protect these systems from increasingly sophisticated attacks have become critically important to the Department and each of its subordinate organizations. The certification and accreditation (C&A) process, required by Federal law and Departmental guidance, is designed to ensure that the agency's information systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The process involves determining whether system controls are in place and operating as intended, identifying weaknesses, mitigating them to the maximum extent possible, and officially recognizing and accepting residual risks. C&A's must be performed on all systems, and they remain in force for a three-year period unless significant changes are made to the system or operating environment.

Previous Office of Inspector General reports have disclosed shortcomings with the Department's C&A process. These reports identified several sites that had incomplete C&A processes as well as sites that failed to comply with National Institute of Standards and Technology (NIST) requirements. Because of these problems, we conducted this audit to determine whether the Department's unclassified information systems had been appropriately certified and accredited for operation. This audit was performed in conjunction with, and expands on, issues that were addressed in our report on the *Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006).

RESULTS OF AUDIT

Despite recent efforts by the Department to improve its process by strengthening guidance, many of its systems were not properly certified and accredited for operation. For example:

- Nine of 14 sites reviewed had not properly assessed the potential risk to their systems and had not adequately tested or evaluated system security controls;
- In many instances, senior agency officials accredited systems even though they had not been provided with adequate or complete risk information;

- Six of the 14 sites examined had not identified the specific residual risk associated with system operation; and,

- At two sites, the role of the Designated Accrediting Authority, the individual responsible for accepting risks associated with system operation and granting authority to operate, had been improperly delegated to a contractor official.

Several issues contributed to widespread problems with the Department's C&A process. In particular:

- Implementing instructions prepared by organizations did not always comply with mandatory NIST C&A guidance; and,

- The Office of the Chief Information Officer and other Departmental organizations did not adequately review completed efforts for quality or compliance with requirements; and,

- Field activities were required to complete internal C&A's within an extremely compressed timeframe.

Without proper C&A, the Department lacks assurance that its information systems and the data they contain are secure.

During our review, we did note that the Department continues to revitalize its Cyber Security Program. The Office of the Chief Information Officer recently issued updated guidance, and the National Nuclear Security Administration (NNSA) is implementing a program to standardize its certification process. In addition, the Office of Science, in conjunction with the Office of Health, Safety and Security, has been conducting site visits to identify and resolve cyber security problems. This process, if implemented across the complex, should help the Department improve its C&A process. While these actions are promising, we made several recommendations designed to strengthen the C&A process and improve the cyber security posture of the Department.

Due to security considerations, specific information regarding the sites and systems with certification and accreditation problems has been omitted from this report.

MANAGEMENT REACTION

The Department concurred with the report's conclusions and recommendations. In particular, management indicated that one of the priorities in Fiscal Year 2007 is to continue to improve the Department's C&A process, bringing it to an acceptable level. Comments submitted by the Department's Chief Information Officer on behalf of his and other offices are included in their entirety in Appendix 3.

In separate informal comments, NNSA noted that it had developed cyber security policies that it believed generally satisfied NIST requirements and that its sites were required to

follow those policies. However, the attached report notes that the NNSA Policy Letters (known as NAPs) do not include certain critical NIST requirements related to the C&A process.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary of Energy
Under Secretary for Science
Chief of Staff
Chief Information Officer

CERTIFICATION AND ACCREDITATION OF UNCLASSIFIED INFORMATION SYSTEMS

TABLE OF CONTENTS

THE CERTIFICATION AND ACCREDITATION PROCESS

Ensuring Information System Security

Our review of 14 sites disclosed that many of the Department of Energy's (Department) information systems were not appropriately certified and accredited for operation. Despite specific guidance from the Department, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB), responsible officials omitted or did not properly complete many of the specific, detailed activities required for certification and accreditation (C&A). In a number of instances, categorizations that drive risk level had not been properly assigned, and risk-specific controls had not been adequately tested. Senior agency officials that accredited systems did so on many occasions without adequate or complete certification documentation and were unable to identify the specific residual risk associated with system operation. In two instances, Federal officials improperly delegated accrediting authorization to a contractor.

Security Categorization and Control Testing

Although specifically required by NIST guidance, security categorizations were not always assigned to systems during the C&A process. These categorizations are used to establish the impact that compromise of the system or loss of information would have and to determine whether systems should be assigned low, moderate, or high risk levels. Security level determinations help identify applicable controls and how they should be incorporated into the system security plan. Risk levels should be established at the highest component level of a system.

Despite the aforementioned requirements, systems at 5 of 14 sites included in our audit lacked both system and information-level categorizations. Four other sites had assigned system and information security categorizations to an entire enclave or group of systems without regard to the varying security levels of systems in the enclave. One of these enclaves contained systems processing data at a high risk level, while the security categorization selected resulted in them being protected only at the low risk level.

In addition, required evaluations and testing of security controls had not been performed or were inadequate at several sites we visited. NIST guidance requires that organizations evaluate controls, design and execute plans to test identified controls, and document the results of the testing and any corrective actions that are necessary.

Contrary to these requirements, four sites had not prepared security control test plans. Additionally, nine sites did not adequately examine controls in accordance with NIST requirements. For example, the plans lacked several key components, such as testing of all controls and a description of the methods and procedures to be used to conduct the assessment. Had the site officials properly evaluated the system controls, they may have determined the extent to which the controls were implemented correctly, operating as intended, and producing the desired outcome.

Documentation Supporting Certifications

In many cases, accreditation decisions were made without adequate information. Specifically, several critical steps had not been conducted or were not properly documented. In particular:

- System-specific risk assessments, activities required by NIST and Department guidance to identify risks and potential threat sources, had not been conducted at 5 of the 14 sites reviewed. For example, one site had not conducted individual risk assessments on 11 of its 12 major applications and general support systems. Risk assessments, which analyze the nature and level of threats and vulnerabilities, should be conducted at the beginning of the certification process.

- Accreditation boundary information – data necessary to identify all system components – lacked sufficient detail to understand the system and determine the scope of C&A at 6 of the 14 sites visited. The six sites were unable to provide inventories of the hardware and software included within defined accreditation boundaries. As noted in NIST implementing guidance, these inventories are a key initial step in determining what system elements are exposed to residual risk.

- Information showing connectivity between systems, sites, and/or agencies was incomplete at 5 of 14 sites reviewed. For example, at one site, no connection data was available to explain how connections were made to the Department-wide network that the site used for data transmission. Such information is critical to ensure that the site has identified and

mitigated risks such as those involved with connecting to the internet.

- At 4 of 14 sites evaluated, systems lacked required Plans of Actions and Milestones (POAMs) to document and monitor progress to correct security vulnerabilities found during the certification process.

- Contingency plans were not properly tested at 5 of 14 sites reviewed. Such plans detail how to keep a system's critical functions operating in the event of disruptions. The periodic testing of a plan, typically annually, allows officials to uncover, and hopefully, correct flaws in the plan and in its implementation prior to an actual disaster or system disruption.

- System self-assessments had not been conducted at six sites. Self-assessments, required annually by the Federal Information Security Management Act of 2002 (FISMA), provide a method for agency officials to determine the current status of their information security programs and, where necessary, correct deficiencies and establish targets for improvement.

Residual Risk

Six sites reviewed did not specifically identify the residual risks that management accepted by permitting systems to operate. Residual risk is the threat remaining after security measures have been applied to the system. At the time of accreditation, senior agency officials must be able to determine the risk to the Department that results from the operation of the system and accept such risk given the organization's need for the system. At many sites, the amount of residual risk accepted by the accrediting officials was not identified. Further, based on the available certification documentation, senior agency officials would not have been able to determine the residual risk they were accepting prior to accreditation.

Accrediting Authority

At two National Nuclear Security Administration (NNSA) sites, the role of Designated Accrediting Authority (DAA) had been improperly delegated to a contractor official. While the actual DAA assigned to the two national laboratories in question was a Federal employee, the DAA delegated the duties and allowed a contractor official to accredit systems.

While NIST and Departmental requirements allow delegation of duties, they recognize that the authorizing official has inherent U.S. government authority and thus mandates that the accrediting official be a Federal employee. At one site, the contactor official had accredited the financial and human resource systems, each of which contained sensitive privacy and other operational information. By permitting this delegation, Federal officials with cognizance over these sites may not be fully aware of the risks of operating these systems.

Implementation Oversight

Our audit identified several issues that, at least in part, contributed to widespread problems with the Department's C&A process. In particular, implementing instructions prepared by organizations did not always comply with mandatory NIST C&A guidance. The Office of the Chief Information Officer (CIO) and program elements also did not adequately review completed efforts for quality or compliance with requirements. These issues, coupled with extremely compressed completion timelines, adversely impacted the quality and usefulness of efforts to identify and address information security weaknesses.

Implementation of NIST Requirements

Direction from Departmental elements was not always consistent with Federal certification and accreditation requirements. For example, at the direction of the Office of Science, many of its field sites inappropriately applied NIST requirements for categorizing system risk levels and applying corresponding security controls, resulting in systems being protected at a lower level than needed. Similarly, NNSA site officials continued to indicate that they were required to comply with NNSA Policy Letters (known as NAPs), as opposed to meeting NIST requirements. However, our review disclosed that none of the NNSA sites had fully implemented the NAPs and, in fact, sites estimated that it may take from 2009 to 2015 to fully implement such policy. Furthermore, many NNSA field sites were permitted to follow a less thorough certification and accreditation process that did not include all NIST or NNSA requirements. In addition, our comparison of the NAPs to NIST guidance found that while the NNSA certification and accreditation policy generally incorporates NIST guidance, we identified areas where it did not. Specifically, the NAPs do not address certain NIST requirements, such as post-accreditation

monitoring of selected security controls and developing plan of action and milestones.

Quality Assurance and Performance Monitoring

The Office of the CIO and the Departmental elements reviewed did not always have an effective mechanism in place to ensure that documentation prepared and testing performed to support system accreditations met NIST requirements. Department Order 205.1A, *Department of Energy Cyber Security Management*, December 4, 2006, establishes line management accountability through Senior Department management to ensure protection of information systems. While NNSA and the program offices generally took action to ensure C&As were performed, they did not have an effective process in place to evaluate the quality of the efforts. For example, NNSA did not have a process that monitored their field site C&A activities.

Similarly, when we initiated our review, the Office of Science did not actively oversee site C&A activities. However, concurrent with our review, the Office of Science began its Site Assisted Visit initiative. Computer security specialists from the Office of Science and the Office of Independent Oversight, Office of Health, Safety, and Security conducted joint visits to 12 of the Office of Science's 15 sites to identify cyber security weaknesses, develop corrective action plans, and follow up to ensure corrective action was taken. We believe this initiative, if fully implemented and deployed across the complex, should result in significant program improvements. The effort is currently limited to mostly Office of Science sites, and while two sites outside of the Office of Science were reviewed, there are no immediate plans to expand the initiative to other program elements.

The Office of the CIO also had not regularly performed independent verification and validation (IV&V) activities essential to evaluating the adequacy of Cyber Security Program performance. While we learned that some IV&V work was performed during Fiscal Year (FY) 2005 on selected system certifications and accreditations, findings from these efforts were never remediated. Officials from the Office of the CIO explained that they informed responsible program officials of deficiencies identified, but those program officials had taken no other action to ensure that the findings were resolved. Although Office of the CIO officials

indicated that no additional review work in that area had been performed, they also told us that they intended to perform a review of a sample of certification and accreditation packages during 2006. However, at the time of our review, management informed us that it was unable to complete the planned reviews because of other pressing concerns.

Compressed Implementation Schedule

In some cases, officials told us that extremely compressed timeframes imposed by the Department for performing C&As prevented them from doing a thorough job. Since its inception in 2002, FISMA required that the Department's major systems and general support systems be certified and accredited before being placed into operation. The Department initially reported to OMB in its FY 2003 FISMA report that about 83 percent of its systems were accredited. However, our concurrent review at that time found that only 26 percent of the systems were properly certified and accredited. To address this situation, and in preparation for FY 2004 FISMA reporting, the Department set a deadline of June 30, 2004, to certify and accredit 90 percent of its systems. This goal, according to the Department officials, required program offices and field sites to work more quickly than feasible, and one site official acknowledged that it became a "paperwork process" rather than a thorough review of the systems. In a few instances, officials acknowledged that their C&A packages lacked some key components. Despite a number of reviews noting problems, many of these incomplete or inadequate efforts had not been updated or re-performed, and sites continue to rely on them.

System Security and Reporting Assurance

Without proper C&A of systems, the Department lacks assurance that its systems and data are secure. In addition, certifying and accrediting officials may lack sufficient information to make an informed decision regarding authorizing systems for operation and to accept the residual risk to agency operations. As noted in NIST 800-37, "*it is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.*" Inadequate C&A of systems leaves valuable information technology resources potentially vulnerable to cyber attacks from internal and external sources and could result in data tampering, disruption of critical

operations, and inappropriate disclosure of sensitive information.

Also, without a consistently applied C&A process, the Department has no assurance that it is correctly reporting its FISMA submissions. For example, in FY 2006, the Department reported to OMB that 99.8 percent of its systems were certified and accredited. As noted in our report, however, many of the efforts were of poor quality and did not satisfy a number of protection goals. Additionally, our review found that the process followed by several sites was inconsistent and lacking in a number of critical areas. Consequently, we believe that the number of systems certified and accredited in accordance with Federal regulations is significantly lower.

RECOMMENDATIONS

Consistent with recommendations made in our report on the *Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006) and to ensure the Department's information systems are properly certified and accredited for operation, we recommend that the Administrator, National Nuclear Security Administration, the Under Secretary for Science, and the Under Secretary of Energy, in conjunction with Office of the Chief Information Officer:

1. Ensure that program and site guidance includes all certification and accreditation requirements set forth by NIST and OMB;

2. Evaluate the Office of Science's Site Assisted Visit initiative for feasibility of expanding this or a similar oversight process across the complex; and,

3. Ensure that system accreditations and re-accreditations are conducted in a timely manner to properly secure the Department's information system resources, to include correcting problems with existing C&As that we identified.

MANAGEMENT REACTION

The Department concurred with the report's conclusions and recommendations. In particular, management indicated that one of the priorities in Fiscal Year 2007 is to continue to improve the Department's C&A process, bringing it to an acceptable level. Comments submitted by the Department's

CIO on behalf of his and other offices are included in their entirety in Appendix 3. In separate informal comments, the NNSA indicated however that its sites were not required to implement NIST requirements. NNSA noted that it had developed NNSA Policy Letters (known as NAPs) that it believed generally satisfied NIST requirements and that its sites were required to follow those policies.

NNSA officials attributed the accreditation of systems without adequate or complete documentation to the lack of understanding, training and education of some senior agency officials. Additionally, NNSA requested more detail on the conditions cited in the report, specifically the findings relevant to security categorizations, residual risk, and improper delegation of accrediting authority.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations. We do not, however, agree with arguments advanced by NNSA in its informal comments. In particular, we disagree with NNSA's assertion regarding the adequacy of its policy and its contention that it does not have to explicitly comply with NIST requirements. As we identified in our report, the NAPs do not include certain critical NIST requirements related to C&A. Office of Management and Budget implementing guidance for FISMA specifically requires that organizations comply with NIST guidance.

Should an organization elect to develop and adopt its own cyber security guidance – as NNSA has done – FISMA requires that the organization affirmatively demonstrate that all NIST requirements are incorporated in such locally developed guidance. Even if NNSA's argument that its internally developed procedures address all NIST requirements is accepted, problems would still likely exist because many of NNSA's sites have made little progress in implementing its cyber security policies. In one recent and particularly noteworthy example, we noted in our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory*, (November 2006) that the Laboratory had made little progress in complying with NNSA's NAPs. In this instance, the Laboratory's lack of progress in this area adversely affected computer security and contributed to the unlawful diversion of classified information from one of its networks.

Specific details of our findings were provided to both NNSA Headquarters and relevant site officials. In addition, details will be provided again in reports we are issuing separately to NNSA Headquarters. Due to the nature of the conditions, specific details on vulnerabilities and locations have been omitted from this report.

Appendix 1

OBJECTIVE

To determine whether the Department had appropriately certified and accredited its systems.

SCOPE

The audit was performed between September 2005 and August 2006 at Departmental Headquarters in Washington, DC, and Germantown, MD; NNSA Service Center and Sandia National Laboratory in Albuquerque, NM; Lawrence Berkeley Laboratory in Berkeley, CA; and Oak Ridge National Laboratory, the Oak Ridge Office, the Y-12 National Security Complex, and the East Tennessee Technology Park in Oak Ridge, TN. In addition, we incorporated findings regarding the certification and accreditation process at Argonne National Laboratory and Chicago Office in Argonne, IL; Fermi National Accelerator Laboratory in Batavia, IL; Kansas City Plant in Kansas City, MO; Los Alamos National Laboratory in Los Alamos, NM; and the Nevada Test Site in Mercury, NV.

METHODOLOGY

To accomplish our evaluation objective, we:

- Reviewed applicable laws and directives pertaining to the certification and accreditation of information technology resources, including the Federal Information Security Management Act, Office of Management and Budget Circular A-130 (Appendix III), DOE Order 205.1, and DOE CIO Guide 205.1-2;
- Reviewed applicable standards and requirements issued by NIST;
- Reviewed the Department's overall certification and accreditation guidance and practices throughout the organization;
- Held discussions with field site officials and officials from various Departmental offices; and,
- Reviewed reports by the Office of Inspector General and the Government Accountability Office.

We also evaluated the Department's implementation of the *Government Performance and Results Act* and determined that it had established performance measures for system

certification and accreditation. We did not extensively rely on computer processed data to satisfy our audit objective.

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 certification and accreditation of information 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 Department officials on December 13, 2006.

RELATED REPORTS

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0748, December 2006). Cyber security is one of seven challenge areas facing the Department of Energy. Several Office of Inspector General (OIG) reports have highlighted the need for improvements in the Department's overall cyber security program. For example, during the annual FISMA review, the OIG found that, among other things, many certification and accreditations had not been performed or were inadequate and contingency planning had not been completed for certain critical systems.

- *Special Inquiry Report to the Secretary: Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006). As a result of the report of the removal of classified information at Los Alamos National Laboratory (Laboratory), the Secretary requested that the Office of Inspector General conduct an investigation. The report noted that the security framework relating to the incident at the Laboratory was seriously flawed. Specifically, the review disclosed that (1) in a number of key areas, security policy was non-existent, applied inconsistently, or not followed; (2) critical security internal controls and safeguards were not functioning as intended; and (3) monitoring by both Laboratory and Federal officials was inadequate.

- *The Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006). The report noted that weaknesses continue to exist that expose its critical systems to an increased risk of compromise. For example, many system C&As had not been performed or were inadequate in that they lacked essential elements such as annual self-assessments and independent testing of security controls. Specifically, at four sites, seven systems were identified, some of which were core operational systems, for which the C&A process had not been completed. At 12 sites, while organizations provided documentation supporting completion of the C&A process, the report noted that many specific, detailed activities required by NIST guidance were not performed.

- *The Department's Unclassified Cyber Security Program – 2005* (DOE/IG-0700, September 2005). The report noted that certification and accreditation of systems and a comprehensive inventory of major systems remain incomplete. The review identified various problems with the certification and accreditation packages including missing Plans of Action and Milestones, risk assessments, security plans, and/or a lack of accreditation documentation.

- *Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements* (GAO-05-552, July 2005). The report noted pervasive weaknesses in the major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of Federal

information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; continuity of operations planning was often inadequate; and security programs were not fully implemented at the agencies. These weaknesses existed primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put Federal operations and assets at risk of fraud, misuse, and destruction. In addition, they placed financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

- *Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation* (GAO-04-376, June 2004). The report noted that NIST had provided guidance for the certification and accreditation of Federal information systems. The guidance includes new guidelines just issued by NIST, which emphasize a model of continuous monitoring, as well as compliance with FISMA-required standards for minimum-security controls. Many agencies report that they have begun to use the new guidance in their certification and accreditation processes. However, the review of documentation for the certification and accreditation of 32 selected systems showed that these criteria were not always met. Further, some agencies did not have routine quality review processes to determine whether such criteria are met.

Department of Energy
Washington, DC 20585

November 21, 2006

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR
FINANCIAL, TECHNICAL, AND CORPORATE
AUDITS

FROM: THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER

SUBJECT: Comments on the Draft Report on "The Department's Certification and Accreditation of Information Systems," IG-32 (A05TG045)

Thank you for the opportunity to review and comment on the Draft Report on *The Department's Certification and Accreditation of Information Systems,* dated September 25, 2006. The Office of the Chief Information Officer (OCIO) concurs with the report's conclusions and recommendations.

As part of the ongoing revitalization of the Department's cyber security program, we are taking steps to ensure that DOE policy clearly requires that the cyber security guidance issued by NIST as well as relevant OMB directives are to be followed within the Department. Implementation of this requirement will be achieved in significant part by incorporating key NIST guidance in our OCIO guidance and in updated Program Cyber Security Plans to be issued by the Under Secretaries and others.

We are also planning an appropriate cyber security compliance review program and a DOE-wide outreach effort that builds on the successes of the Office of Science's Site Assistance Visit initiative. In carrying out this year's cyber security efforts, we will be giving special attention to ensuring that the detailed findings summarized in this Draft Report are thoroughly addressed. One of our priorities in FY 2007 is to continue to improve DOE's certification and accreditation processes, bringing these processes up to an acceptable level.

OCIO looks forward to working with the Under Secretaries to implement the recommendations in this report, and we will keep your office advised of our progress. If you have any questions or need additional information about this response, please give me a call, at (202) 586-0166, or contact Associate CIO for Cyber Security Bill Hunteman, at (202)-586-4775.

IG Report No. DOE/IG-0752

CUSTOMER RESPONSE FORM

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

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

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

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

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

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

Name _____ Date _____

Telephone _____ Organization _____

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

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

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact 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.doe.gov

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