



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

Special Report

The Department's Unclassified Foreign Visits and Assignments Program



Department of Energy

Washington, DC 20585

March 24, 2008

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Special Report on "The Department's
Unclassified Foreign Visits and Assignments Program"

BACKGROUND

The Department of Energy's national laboratories and various Federal officials interact with thousands of foreign national visitors and assignees every year. Visits and assignments are for a variety of purposes, including research collaborations and access to scientific user facilities. While the Department reports that these interactions stimulate ideas and foster research, they also carry inherent security risks. The Office of Foreign Visits and Assignments and the Office of Intelligence and Counterintelligence help the Department ensure that security risks are addressed while fostering collaboration with foreign nationals.

In our report on *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 2002), we observed that the Department had not adequately controlled unclassified visits and assignments by foreign nationals. That audit identified issues such as admitting visitors prior to receiving required approvals, not completing background checks, and neglecting to enter appropriate and accurate information into the Department's Foreign Access Central Tracking System (FACTS). Management agreed to take corrective action and has since issued a new Department order to govern these activities. Due to the sensitivity of the program and the potential for harm, we initiated this review to determine whether the Department had improved the management of its Foreign Visits and Assignments Program.

OBSERVATIONS AND CONCLUSIONS

The Department had addressed several previously reported issues. Additional and continuing weaknesses, however, diminished the effectiveness of controls designed to reduce the security risk associated with foreign visits and assignments. In particular, hosts for foreign nationals – individuals responsible for the day-to-day management and security associated with visits or assignments – had not ensured that a number of protective measures were implemented. For example, certain hosts did not always:

- Take action to ensure that site or facility access was terminated when the foreign nationals completed visits or assignments. In one extreme case, we found that a visitor, whose assignment had been revoked, did not have his access authorization cancelled and was able to enter the former host facility after normal operating hours without being discovered;



- Familiarize themselves with or enforce specific security plans – plans designed to restrict movements, activities and/or access – for visitors they were assigned to host from sensitive countries such as China and India;
- Verify the identity and validity of foreign nationals' immigration status information prior to or periodically during assignments or visits as required for off-site visits; and,
- Ensure that required counterintelligence reviews were conducted prior to permitting foreign nationals to access sensitive information systems and data.

We also identified a significant and continuing problem with the maintenance and accuracy of FACTS that detracted from the Department's ability to track the immigration status or other factors for its many foreign visitors and assignees. Specifically:

- For 104 of the 188 (approximately 55 percent) randomly selected FACTS visits or assignments we reviewed, tracking information was not properly entered, contained errors, or was not up-to-date.

When viewed collectively, these problems or programmatic shortcomings caused us to conclude that security risks associated with the Department's Foreign Visits and Assignments Program remain higher than necessary. Contractor operated laboratories had not ensured that hosts were cognizant of their responsibilities and were performing them properly. Those laboratories and the Office of Foreign Visits and Assignments also had not taken sufficient steps to ensure that data in the FACTS was reliable. Problems with recordkeeping and tracking could limit the Department's ability to provide accurate and/or complete foreign national information to law enforcement agencies.

To its credit, the Department had addressed a previously identified issue – ensuring that foreign nationals had current passports and visas for on-site visits and assignments. Yet, we concluded that more needs to be done to reduce the risk that individuals harboring malicious intent could access sensitive information or damage facilities. Thus, the attached report includes several recommendations designed to address the problems noted in our review.

We also noted another matter for consideration pertaining to cyber access controls at one National Nuclear Security Administration (NNSA) laboratory. This matter is discussed more fully in Appendix 2 of the report.

MANAGEMENT COMMENTS

Management generally concurred with our findings and recommendations and in certain instances indicated that corrective actions had been initiated. NNSA submitted informal comments and indicated that it would develop corrective actions and monitor progress to completion. Formal Management comments are included as Appendix 4.

Attachment

cc: Acting Deputy Secretary
Administrator, National Nuclear Security Administration

Under Secretary of Energy
Under Secretary for Science
Chief of Staff

SPECIAL REPORT ON THE DEPARTMENT'S UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS PROGRAM

TABLE OF CONTENTS

Management of Unclassified Foreign Visits and Assignments

Details of Finding	1
Recommendations.....	7
Comments	8

Appendices

1. Objective, Scope, and Methodology.....	9
2. Other Matter for Consideration.....	11
3. Prior Reports	12
4. Management Comments	13

MANAGEMENT OF UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS

Tracking and Hosting Foreign Nationals

Weaknesses in hosting and tracking diminished the effectiveness of the Department of Energy's (Department) Foreign Visits and Assignments Program. In particular, our review of foreign visits at four laboratories and two Headquarters offices revealed that foreign national hosts were not performing a number of required tasks. Specifically hosts did not always: (1) take action to ensure that site or facility access was properly and promptly terminated when the visit or assignment was completed; (2) become familiar with and ensure that visitors or assignees complied with individualized security plans; (3) verify the identity and validity of foreign nationals' status information for off-site visits as required; and, (4) ensure that counterintelligence reviews were completed prior to permitting foreign nationals to access sensitive information systems and data. We also noted that a significant and continuing problem with the maintenance and accuracy of the Department's Foreign Access Central Tracking System (FACTS) had not been resolved.

Host Responsibilities and Actions

To help reduce risk, the Department requires that a host be appointed to define and control the work and access of each visitor or assignee. Hosts are responsible for the successful conduct of the foreign visit, including keeping site officials informed of the visit or assignment status; ensuring tracking systems are kept up-to-date with accurate and complete information; and complying with visitor-specific security plans. In addition, in certain cases such as at off-site meetings, the host must obtain and/or validate foreign national status documentation, i.e. visas and passports. These required actions are particularly important because nearly all of our sampled visitors represented countries such as the People's Republic of China, India, and Russia – states that are considered "sensitive" because of national security, nuclear nonproliferation, or terrorism support concerns. As detailed in the following paragraphs, however, we discovered that hosts were often not always aware of the full scope of their duties or mistakenly believed that other organizations or individuals were responsible for satisfying security requirements.

Updating Visit or Assignment Status

Hosts at various sites told us that they had not always kept site officials informed of the status of visits or assignments as required. Many of the hosts stated that even though they were aware that a particular collaboration had ended or a need to visit a user facility no longer existed, they had not notified Foreign Visits and Assignments Program managers that the visit should be closed out and facility access terminated. We found, based on host interviews at one laboratory, that 14 of the 27 foreign nationals selected for review no longer needed site access because the visit or collaboration had been completed. For example, one assignee no longer needed access to the user facility at a particular laboratory because he was conducting his research at another laboratory. In another case, an assignee, that accepted a job in Italy, had reportedly departed the United States and was no longer involved in a project with the laboratory. Another host told us that a particular assignee had completed the work and the collaboration was no longer necessary.

Security Plans

Hosts were not always cognizant of and did not enforce security plans designed to restrict the access and/or scope of the visitor or assignee. For visitors and assignees from sensitive countries, a specific security plan must be developed for each foreign national. These security plans are required to address concerns such as the type of security area to be visited and types of information to be accessed. Four of the nine hosts interviewed at one Office of Science (Science) laboratory advised us that they did not have a specific security plan in their possession nor were they otherwise familiar with the content of the security plan. At another Science laboratory, 12 of 23 hosts indicated that they were unfamiliar with the specific security plans for their visitors. At both locations, many hosts said that individual security plans were maintained by an administrative staff member in their division, but the security plans were neither provided to nor read by the host.

Validating Status Documentation

At one National Nuclear Security Administration (NNSA) laboratory and one Headquarters office, hosts were not

always obtaining and/or validating status documents such as passports and visas for foreign visitors as required. Hosts for visitors at the NNSA laboratory were specifically required to take these actions for visitors or assignees not physically working at the laboratory; i.e., those involved in collaborations at off-site locations. In some cases, hosts arranged for this class of visitor or assignee to obtain remote access to the laboratory's information systems. Hosts are responsible for obtaining and providing up-to-date status documents to the foreign visits office in these instances and also examining previously-provided information to validate the identity of foreign nationals.

At the NNSA site where foreign visitors were involved in off-site collaborations, hosts were not always obtaining immigration status information from foreign visitors. In three of four cases we reviewed involving off-site collaboration, the hosts indicated that they did not obtain up-to-date status information for visitors, nor did they provide the information to the foreign visits office. These hosts also did not visually inspect status documents. As a result, status information for these visitors did not exist or was not accurate in either the site foreign visitor tracking database or FACTS and it was uncertain that the foreign nationals were in valid status for the duration of the visit or assignment.

During our testing at one Headquarters office, we also learned that despite Departmental security requirements to the contrary, hosts were not required by that office to visually inspect and verify passport and visa information at the time of foreign visitor arrival at Headquarters facilities. Obtaining and validating up-to-date status documents ensures that passport and visa information is correct before allowing access to Department facilities and is important to demonstrate that an individual's identity and authority to work are valid, access for certain activities is appropriate, and the foreign national is eligible to be in the United States. During the course of our review, the Headquarters office in question acknowledged this weakness and immediately mandated the verification of passport and visa data.

Access to Sensitive Data

At one NNSA laboratory, some hosts were not providing necessary information to ensure that required

counterintelligence reviews were conducted prior to permitting foreign nationals to access sensitive information systems and data. Department directives mandate that a counterintelligence review must occur for all foreign nationals who have access or potential access to sensitive information. Such information may reside on computer systems and could include categories of unclassified controlled information such as export control, proprietary, or unclassified controlled nuclear information. Hosts did not always ensure an annotation was made in the "sensitive" subject field of the laboratory's foreign national tracking system – an action that would automatically trigger the performance of needed national indices checks and local counterintelligence reviews.

Centralized Tracking

Similar to the issue identified in *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 2002), laboratories were still not ensuring that the Department's official complex-wide database for tracking all foreign national visitors and assignees was current and complete. Biographical and personal information, including passport and visa information, for each foreign visitor, is required to be entered by field sites into FACTS, the Department's official database. Such information contains identification numbers and passport and visa expiration dates and is critical because visitors are not authorized to be in the United States without current credentials. While field sites are allowed to maintain their own tracking systems, FACTS is the only foreign visitor tracking database authorized by the Department and is the official source used to report information to Congress and other stakeholders. Because sites are maintaining their own systems, the Department permits sites to upload data to the FACTS from site-level tracking systems to eliminate the burden of duplicate entry. Our analysis, however, established that three of the four national laboratories in our review were not ensuring that site-level information was correct in FACTS.

Testing of FACTS data for one NNSA and two Science laboratories revealed significant and continuing problems with the accuracy of legal status documentation, such as visa and legal permanent resident information. For 104 of the 188 randomly selected visitors we reviewed, all of

which were from sensitive countries, tracking information was not properly entered, contained errors, or was not up-to-date. Specifically, 53 of the 58 sampled visitors at an NNSA laboratory, 32 of 64 sampled visitors at one Science laboratory, and 19 of 66 sampled visitors at another Science laboratory either contained no legal status information or such data was out-of-date.

Additionally, the three laboratories were not ensuring that visits were closed in FACTS within the prescribed 15 day timeframe. Of the 179 completed visits we evaluated, 96 had not been closed within the prescribed time period. The table below illustrates the number of days taken to officially close each visit associated with our sampled foreign national visitors.

Number of Days to Close Visit or Assignment				
	15 or Fewer	16-90	Over 90	Total
Science Laboratory	23	19	11	53
Science Laboratory	19	17	0	36
NNSA Laboratory	41	12	37	90
Totals	83	48	48	179

It is important to note that 24 visits or assignments remained open for more than a year after they should have been closed.

In a related issue, at both of the Science laboratories, visitors and assignees were often given access to the sites for a two-year time period although they may or may not be at the site for that entire duration. This practice was used primarily to accommodate visits to user facilities for which actual visit dates were unknown at the initiation of the visit or assignment. In many cases, the purpose for the initial visit may be accomplished in less time, but the visit is not "closed" until the end of the two-year period. As a consequence, visitors or assignees unnecessarily retain their security badges and have the ability to access the site for the entire two-year period.

**Departmental Foreign
National Tracking
and Hosting
Requirements**

Hosting and tracking weaknesses existed because: (1) site foreign visits and assignments managers were not validating that hosts were meeting established requirements; and, (2) neither field sites nor Headquarters officials were conducting basic data comparisons.

Validating Host Activities

Although host-specific training existed, laboratories in our review were not validating that hosts were effectively fulfilling their responsibilities. Each of the laboratories required specific training to qualify individuals to host foreign nationals. Training generally covered requirements regarding notification of visit or assignment end dates, familiarity with specific security plans, and information hosts should be providing, such as a need for access to sensitive information. While all hosts we interviewed had received the applicable training, they were not meeting many of their hosting requirements and responsibilities.

Data Comparisons

Organizations also did not take action to ensure that foreign visit information was correct and/or periodically reconciled. Based on the extensive differences identified in our comparison of site-level foreign visit information to data in FACTS, we concluded that field sites were not conducting basic comparisons of data maintained in their own tracking systems to that in FACTS. Our work demonstrated that even basic visual data checks – such as comparing the expiration dates of visas between the systems – would have revealed inadequacies with data in FACTS. Further, while FACTS had the capability to sort and search data, the Office of Health, Safety and Security's (HSS) Office of Foreign Visits and Assignments had not built basic edit checks into FACTS and was not otherwise using program tools to identify problems such as visa expiration dates that preceded end visit dates or visits that did not have visa information at all. For example, a review of FACTS data from one Office of Science site revealed that visas for 15 of 66 visitors in our sample had expired before their visits even began.

**Mitigating Security
Risks**

Weaknesses in the Department's foreign visits and assignments program increase the security risk for the Department's facilities and information. For example, at least one visitor accessed a laboratory using a valid identification badge on two occasions the month after his

assignment had been revoked. Site officials were unaware of the unauthorized access until we brought it to their attention.

The unauthorized access is exacerbated by the fact that the same visitor's background check had expired four months prior to the two unauthorized visits, which were made after the site's normal operating hours. Due to the fact that foreign national maintained an active visit and security badge in laboratory systems, he was able to access the site without question. Neither the host nor other site officials could explain his purpose or whereabouts on the site. The situation could have been avoided had the visit been closed and site access terminated at the same time the assignment was revoked.

While the Department must adhere to its mission to foster and advance scientific research and development, minimizing risks is important because the national laboratories hold some of our most valuable national security assets. Research essential to our national defense relies increasingly on unclassified science and technology, and thousands of foreign nationals from institutions around the world interact with laboratory employees at Department facilities. While we recognize that documenting and tracking foreign national visitors and assignees requires additional attention and effort at the site-level, the risk or damage to the Nation's security interests demand vigilance. The Department must ensure that it maintains needed information and is prepared to respond to inquiries in a timely manner.

RECOMMENDATIONS

To help ensure that Department requirements for foreign national accountability, access and control are comprehensively detailed and consistently applied, we recommend that the Administrator, NNSA and the Under Secretary for Science require that field sites:

1. Ensure hosts are meeting requirements for updating visit status, familiarizing themselves with specific security plans, validating status documentation as necessary, and providing full details of required sensitive information access;

-
2. Take immediate action to close completed visits or assignment in FACTS and terminate access to sites and facilities that is no longer required; and
 3. Ensure required foreign visitor and assignee information is accurate and complete in FACTS.

To help ameliorate increased risks associated with foreign national interaction and ensure that complete status information is available, we recommend that the Chief Health, Safety and Security Officer:

4. Require that the Office of Foreign Visits and Assignments implement data comparisons, including edit checks and/or error reports generated on a periodic basis, to help ensure that information entered into FACTS is accurate and complete.

MANAGEMENT REACTION

Management agreed with the information in the report and generally concurred with each of the specific recommendations. In a joint response, the Offices of Science and HSS provided comments on intended actions. Science is taking immediate action to work with its Integrated Support Center to close visits and assignments that are no longer required. Additionally, Science will work closely with field sites and HSS in implementing the additional recommendations. HSS responded that its Office of Foreign Visits and Assignments had already begun development of a FACTS modification to add edit checks and error reports to reject the entry of inaccurate and/or incomplete information. In its informal comments, NNSA indicated that it concurred with the findings and recommendations and pledged to take necessary corrective actions. It did not, however, provide a corrective action plan.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations.

Appendix 1

OBJECTIVE

The objective of our review was to determine whether the Department of Energy (Department) had improved the management of its Foreign Visits and Assignments Program.

SCOPE

The review was performed at Headquarters and four national laboratories, two managed by the Office of Science (Science) and two managed by the National Nuclear Security Administration (NNSA), from August 2006 through February 2008. The universe of our samples consisted of foreign national visitors, assignees, and employees at those sites from October 2004 through May 2007.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Department and site-specific policies, procedures, and training materials related to unclassified foreign national visits and assignments;
- Reviewed lists of foreign national visitors, assignees, and employees provided by the Department's Foreign Access Central Tracking System, site badge systems, and site foreign visits and assignment systems;
- Randomly selected samples of 66 sensitive country foreign national visitors, assignees, and employees from one Science-managed laboratory, 64 from the other Science-managed laboratory, and 58 from the NNSA-managed laboratory;
- Judgmentally selected a sample of 100 sensitive and non-sensitive country foreign national visitors and assignees from the other NNSA-managed laboratory;
- Randomly selected samples of 55 and 54 visitors and assignees from each of the Headquarters offices selected for review;
- Reviewed supporting documentation for our sample of foreign national visitors, assignees, and employees;
- Interviewed officials from the Headquarters Office of Foreign Visits and Assignments, Counterintelligence, and selected site security, foreign visits, and Counterintelligence offices to gain and understanding of roles, responsibilities, and procedures; and,

- Interviewed officially-designated foreign national hosts judgmentally selected from our samples to obtain supporting information on visitors or assignees.

We assessed performance measures established under the Government Performance and Results Act of 1993. While specific performance measures concerning foreign visits and assignments did not exist, performance in this regard was either measured by each laboratory's safeguards and securities reviews or will be enhanced with the implementation of our recommendations and suggestions.

Management waived an exit conference.

OTHER MATTERS FOR CONSIDERATION

In addition to weaknesses identified in the overall unclassified Foreign Visits and Assignments Program discussed in this report, we also identified an additional cyber-specific issue at one of the National Nuclear Security Administration (NNSA) laboratories in our review. Specifically, the laboratory had not fully mitigated the risk of foreign nationals gaining unauthorized access to its unclassified Intranet.

Officials at one NNSA laboratory indicated that security features on many laboratory desktop and laptop computers used by foreign national visitors and assignees were not always implemented. We learned from laboratory security officials that software controls designed to prevent foreign nationals from circumventing security features were implemented on laboratory computers assigned to sensitive country foreign nationals. These controls were not, however, implemented on most computers assigned to non-sensitive country foreign nationals. According to officials, users circumventing security features on computers could modify log-on settings, load unauthorized software, remove software, and change computer settings – ultimately permitting unauthorized access to the laboratory's information systems.

Laboratory officials also revealed that some foreign visitors and assignees enjoyed unsupervised use of their foreign government, university, or business laptops in laboratory facilities with live Intranet connections. Both Department and laboratory policy allows both U.S. citizens and non-sensitive country foreign nationals to bring their government, business, or university laptop computers on to the site for unclassified, stand-alone use. Counterintelligence officials at the laboratory told us that they were concerned with the current practice because foreign nationals could connect their computer equipment to the laboratory's Intranet without authorization. These connections pose a threat and could permit the foreign nationals to download large amounts of data, probe the network for vulnerabilities, and implant malicious code.

SUGGESTIONS FOR IMPROVEMENT

To help decrease the risk associated with foreign national data access and computer operation, we suggest that NNSA require the laboratory to:

1. Strengthen security and access controls for computers operated by foreign nationals to help prevent or detect unauthorized or malicious use; and,
2. Specifically restrict the connection of all non-U.S. Government owned equipment to the laboratory's network and Intranet.

PRIOR REPORTS

Office of Inspector General

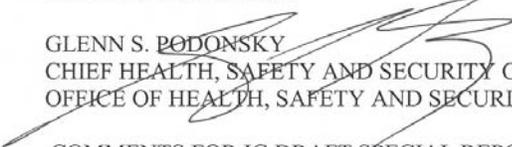
- *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 2002). That audit identified three deficiencies in adequately controlling unclassified visits and assignments at two national laboratories. Those deficiencies included failures to ensure that: (1) all foreign nationals had current passports and visas; (2) foreign nationals were not granted site access prior to official approval and before background checks or counterintelligence consultations were completed; and, (3) sufficient information was provided to the Department of Energy's (Department) centralized tracking system, which was designed to facilitate complex-wide tracking of the status of foreign nationals.
- Our office conducted a series of annual Inspections from 2000 – 2006 of export licensing controls in the Department. These inspections were also part of an effort with other agencies that conduct these activities such as Commerce, Defense, and Homeland Security. The most recent inspection, *The Department of Energy's Review of Export License Applications for China* (DOE/IG-0723, April 2006), concluded that the export license review process to control the export of critical technologies to China was appropriate and consistent with existing procedures. However, it also noted that access by Department officials conducting license reviews to end user-review information maintained by one National Nuclear Security Administration laboratory could be improved, and included a recommendation to address the concern. Additionally, it reported that 12 of 15 recommendations made in the earlier Inspections had been closed, but that export control guidance still needed to be consistently implemented throughout the Department complex and appropriate action was necessary to ensure that licensing officers have access to and proper training in the use of the Department of Commerce's Export Control Automated Support System.



Department of Energy
Washington, DC 20585

March 10, 2008

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM:  GLENN S. PODONSKY
CHIEF HEALTH, SAFETY AND SECURITY OFFICER
OFFICE OF HEALTH, SAFETY AND SECURITY

SUBJECT: COMMENTS FOR IG DRAFT SPECIAL REPORT: The
Department's Unclassified Foreign Visits and Assignments
Program (AO6PT037)

The Office of Health, Safety and Security (HSS) has reviewed the subject draft special report provided by the Office of the Inspector General (IG) on February 15, 2008. The following consolidated response was developed between the Office of Science (SC) and HSS. Both offices support the recommendations of the subject audit and draft report. Below are the responses to the findings and recommendations.

SC generally concurs with the three recommendations presented in the draft report directed to that office to require that field sites:

1. Ensure hosts are meeting requirements for updating visit status, familiarizing themselves with specific security plans, validating status documentation as necessary, and providing full details of required sensitive information access;
2. Take immediate action to close completed visits or assignment in Foreign Access Central Tracking System (FACTS) and terminate access to sites and facilities that are no longer required; and,
3. Ensure required foreign visitor and assignee information is accurate and complete in the Department's FACTS system.

SC will continue to work closely with their field sites and HSS to address these three recommendations. Upon receipt of the final report, SC will respond within thirty days from the date of the final report. As these three recommendations involve both a large database and large numbers of foreign national visitors and assignees, SC will require time in the field to make actions to address these recommendations credible. SC is currently working with the SC Integrated Support Center to close any visits or assignments that are no longer required.



Printed with soy ink on recycled paper

Appendix 4 (continued)

HSS generally concurs with the recommendation in the draft report directed to that office to:

4. Require that the Office of Foreign Visits and Assignments implement data comparisons, including edit checks and/or error reports generated on a periodic basis, to help ensure that information entered into the FACTS system is accurate and complete.

The HSS Office of Foreign Visits and Assignments has begun development of a FACTS system modification to add edit checks and error reports to reject the entry of inaccurate and/or incomplete information into the system. In addition, HSS will continue to work with sites and oversight organizations to ensure reconciliation between FACTS and site-level tracking systems.

If you have any questions, you may contact me on (301) 903-3777, or your staff may contact Ms. Barbara Stone at (301) 903-4642.

cc: Mark Thornock, 31-3
Janet Venneri, SC-41
Richard Speidel, NA-66
Michael Kilpatrick, HS-1
Lesley Gasperow, HS-1.2
Barbara Stone, HS-70
Jennifer Emanuelson, HS-72

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.energy.gov>

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