



U.S. Department of Energy  
Office of Inspector General  
Office of Audits and Inspections

# Audit Report

Security Planning for National  
Security Information Systems at  
Lawrence Livermore National  
Laboratory

OAS-M-11-03

April 2011



**Department of Energy**  
Washington, DC 20585

April 15, 2011

MEMORANDUM FOR THE ADMINISTRATOR, NATIONAL NUCLEAR SECURITY  
ADMINISTRATION

FROM: Rickey R. Hass  
Deputy Inspector General for Audits and Inspections  
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "Security Planning for National Security Information Systems at Lawrence Livermore National Laboratory"

**BACKGROUND**

The National Nuclear Security Administration (NNSA) is responsible for the maintenance and security of the Nation's nuclear stockpile, management of nuclear nonproliferation activities, and operation of the naval reactor programs. A significant amount of the information related to these mission activities is classified and stored or processed in national security information systems. The Lawrence Livermore National Laboratory (LLNL) maintains various national security systems, ranging from diskless workstations to large supercomputers, which process sensitive and classified information in support of program objectives.

In the past, physical and cyber security controls over sensitive and classified information throughout the Department of Energy (Department) have been areas of concern. For example, the Office of Inspector General *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory* ([OAS-SR-07-01](#), November 2006) disclosed weaknesses that contributed to the compromise of classified data. In addition, our report on *Certification and Accreditation of the Department's National Security Information Systems* ([DOE/IG-0800](#), August 2008) identified that enhancements were needed at numerous sites, including LLNL, in the areas of risk management, security planning and contingency planning to reduce the risk of compromise to national security systems. Given the importance of this area, we initiated this audit to determine whether NNSA had developed and implemented an effective risk management process over its national security information systems at LLNL.

**RESULTS OF AUDIT**

Our review found that LLNL had taken steps to improve the risk management process for its national security information systems based on our prior reviews. In particular, officials had initiated actions to address the risks associated with separation of incompatible cyber security duties and the use of mixed-media environments – situations where classified and unclassified systems are co-located. However, we found that additional actions are needed in the area of security planning and policies to reduce the risk of compromise. In particular, we noted that:

- Three of four system security plans we reviewed were incomplete and did not always sufficiently describe security controls and how they were implemented;

- Contractor officials made security-significant changes to national security systems that potentially increased the risk to those systems without first obtaining approval from the Federal Authorizing Official – the person ultimately responsible for accepting risks posed by changes to information systems; and,
- NNSA had not incorporated security controls established by the Committee on National Security Systems, the organization designated by Executive Order 13231 to develop policies and standards for protecting national security information systems, into its cyber security policy, thus negatively impacting LLNL's ability to meet Federal security requirements.

These issues were due, at least in part, to inadequate program and site-level policies and procedures for protecting national security information systems. For example, NNSA cyber security program policies had not been updated since May 2008, and were not aligned with current Federal and Department requirements. The problems identified persisted because of insufficient performance monitoring by Headquarters and Site Office Federal officials. For instance, Federal officials responsible for oversight had not always ensured that changes to systems were appropriate and in accordance with risks identified and accepted as part of the systems' authorization to operate.

Without improvements, the weaknesses identified may limit program and site-level officials' ability to make informed risk-based decisions that support the protection of classified information and the systems on which it resides. LLNL officials reported that they are currently reforming the site's system authorization process and recertifying its national security information systems to better align with current NNSA policies. While these are positive actions, additional effort is necessary. As such, we have made several recommendations that, if fully implemented, should help enhance NNSA's and LLNL's management of risk over national security information systems.

#### MANAGEMENT REACTION

Management indicated that it generally agreed with the report's findings. While the Livermore Site Office did not agree with the report's recommendations, management commented that corrective actions were already underway to address issues identified in the report. However, no specific corrective actions were included in management's comments. In addition, management disagreed with several of the conclusions in the report related to policy implementation and performance monitoring. As appropriate, we modified our report in response to management's comments which are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary  
Associate Deputy Secretary  
Chief of Staff  
Chief Health, Safety and Security Officer  
Chief Financial Officer  
Chief Information Officer

# **REPORT ON SECURITY PLANNING FOR NATIONAL SECURITY INFORMATION SYSTEMS AT LAWRENCE LIVERMORE NATIONAL LABORATORY**

---

## **TABLE OF CONTENTS**

### **Security Planning over National Security Information Systems**

Details of Finding .....	1
Recommendations and Comments.....	6

### **Appendices**

1. Objective, Scope and Methodology .....	9
2. Related Reports .....	11
3. Management Comments .....	12

# **Security Planning for National Security Information Systems at Lawrence Livermore National Laboratory**

---

## **Security Planning over National Security Information Systems**

Our audit found that system security plans for certain national security information systems at Lawrence Livermore National Laboratory (LLNL) were incomplete and did not always sufficiently describe security controls and/or how controls were implemented. In addition, the Livermore Site Office (LSO) Federal Authorizing Official was not always notified when changes that may have been security-significant were made to LLNL's national security systems. We also found that minimum baseline security controls required by the Committee on National Security Systems (CNSS) had not been incorporated into National Nuclear Security Administration (NNSA) policy, thereby impacting LLNL's ability to meet Federal cyber security requirements. As noted in Executive Order 13231, CNSS is the originator of national-level policies and standards for the security of national security information systems.

### Minimum Security Controls

Three of four system security plans we reviewed were incomplete and did not always sufficiently describe security controls and how they were implemented on the systems. Internal oversight organizations have identified similar issues during prior reviews at LLNL and our current review found that these weaknesses had not been fully addressed. For instance:

- LLNL's Security Plan Policy (SPP) which described institutional security controls common to numerous classified information systems was not always complete. For instance, although required by NNSA policy, the plan did not adequately address how records of attempts to access facilities housing classified systems were to be maintained. In another instance, the SPP did not sufficiently describe how fire protection controls had been implemented to prevent or suppress fires. Without a thorough description of how these controls are implemented, security assessors may not be able to design test procedures to determine how effectively controls are being implemented. We noted similar weaknesses for more than 25 controls covering areas such as media protection, system integrity, and system acquisition in the SPP. The issues identified are particularly important in this case because the controls in the SPP are to be implemented on various national security systems across the laboratory.

- 
- Although NNSA policy required that all security controls be identified within security plans by name and description, LLNL plans we reviewed did not always provide this level of specificity. Rather, we found that the security controls documented in three of the security plans we reviewed contained only high-level information about the systems, their boundaries, and how they were protected. However, many of the controls identified did not provide sufficient detail so that an independent security assessor could identify what was required and how the control had been implemented. For example, while the plan for the system containing Secret Restricted Data described diskless computers as having backups performed monthly, it did not identify where, or in what form, the backups were stored or how backups were to be tested for reliability. In preliminary comments on our report, Federal management stated that it had identified similar weaknesses and had directed LLNL to take corrective actions.
  - The Secure Computing Facility (SCF) system security plan also disclosed that affected parties should be notified and the system owner should implement procedures to purchase replacement equipment in the event the SCF systems were unavailable. An SCF official explained that should the LLNL location be deemed unsuitable, NNSA would likely copy the alternate processing site's supercomputer design, which is significantly different from that currently utilized by the system, to re-build the system at the alternate location. The official also stated that, operationally, this made more sense than rebuilding the SCF's unique architecture at the alternate site. However, this course of action and the associated risk-based rationale was not documented in the system security plan; therefore, the Federal Authorizing Official had no opportunity to evaluate the balance of risks and mitigation inherent in this course of action.

#### Managing Changes to System Risk

The Federal Authorizing Official was not always notified when potentially security-significant changes were made to LLNL's national security systems. For example, contractor officials at LLNL made security-significant changes to the Ground-Based

---

Nuclear Explosion Monitoring (GNEM) system without first notifying and obtaining approval from the Federal Authorizing Official – the person ultimately responsible for accepting risks posed by changes. Specifically, 2 of 10 changes made since the system was last authorized to operate in May 2007, were considered security-significant by LLNL contractor officials. We also noted that two additional changes involving physical modifications to the system's accreditation boundary should have been considered security-significant but were not. However, none of these changes had been formally presented to or approved by the Federal Authorizing Official even though they affected the level of risk to the information system. We identified similar issues at LLNL in our previous audit on *Certification and Accreditation of the Department's National Security Information Systems* ([DOE/IG-0800](#), August 2008).

In addition, change control forms completed by contractor officials for the GNEM system stated that the changes had "been reviewed and the implementation is approved for classified data processing under the existing accreditation." However, the National Institute of Standards and Technology (NIST) and NNSA policy both require that only the Federal Authorizing Official is allowed to make risk acceptance and operation decisions. As noted above, none of the 10 change forms had been reviewed and/or approved by the Federal Authorizing Official. During our discussions, the Federal Authorizing Official stated that he was not familiar with the change forms for the GNEM system. Furthermore, in the case of the GNEM system, the security plan had not been updated to reflect and incorporate the security-significant changes identified even though required by NIST. Without timely updates, the Federal Authorizing Official may not have been aware that the GNEM system's components required different security controls because the system had been moved to a new location due to the destruction of the building described in the security plan. Also, we noted that security-significant changes to the Credibility Assessment Network and Protection Planning & Program Support systems were not approved by the Federal Authorizing Official.

#### Incorporation of National-Level Standards

During our audit a separate matter came to our attention that impacted the completeness of system security plans at LLNL. Specifically, we found that minimum baseline security controls required by the CNSS and DOE Order 205.1A had not been

---

incorporated into NNSA policy. Direction issued by CNSS requires that control baselines documented in NIST Special Publication 800-53, Revision 3, be incorporated into system security plans for systems authorized after October 2009. However, we noted that more than 90 security controls and control enhancements related to areas such as access controls and media protection had not been incorporated into the NNSA Policy Letters. As a result, approximately 32 percent of required controls were not required to be documented within the site system security plans or tested as part of the system authorization process. As noted in DOE Order 205.1A, Program Cyber Security Plans are living documents and must be maintained to comply with, among other things, policies promulgated by the CNSS.

**Security Policies and Procedures and Performance Monitoring**

The issues identified were due, at least in part, to inadequate program-level policies for protecting national security information systems. In addition, insufficient performance monitoring by Headquarters and LSO officials contributed to weaknesses not being identified and addressed, as appropriate.

Cyber Security Policies and Procedures

NNSA officials had not established policy that was as stringent as Department of Energy (Department) directives and Federal requirements. In particular, NNSA Policy Letters had not been updated to incorporate revisions to the Federal minimum required security control baselines. We noted that NNSA policy had not been revised since May 2008 and, therefore, did not direct sites to follow current Federal requirements such as CNSS Instruction 1253. In comments on our draft report, NNSA management stated that updates to Department-level directives would require implementation of the CNSS controls. However, management did not provide a timeline for the issuance and implementation of the updated policy. As noted, approximately 32 percent of required controls had not been fully addressed as part of the system authorization process. As LLNL and other NNSA sites are required to follow the NNSA program-level policy, it is important that the policies be updated to reflect current Federal requirements.

Performance Monitoring

NNSA officials at Headquarters and the LSO had not always performed sufficient monitoring of activities involving national security information systems at LLNL. During our discussions with Headquarters officials, we learned that they had not

---

conducted any recent reviews of national security information systems due to competing demands and resource constraints. Rather, Headquarters officials depended on Federal personnel at the sites to provide sufficient oversight. However, we noted that, in December 2009, NNSA imposed a six-month moratorium on assessment activities while a new oversight approach was developed. As a result, no reviews of national security information systems were conducted at NNSA sites until late in Fiscal Year 2010. LSO management noted that it had since conducted a comprehensive survey, and the site was working toward addressing those issues identified during the survey and in our report.

We found that system security plans were incomplete because LLNL officials had not followed NNSA policies that required a thorough description of how all minimum security controls were being implemented. The LSO Federal Authorizing Official stated that the security plans did not provide much detail about the systems because LLNL Information Technology program officials, system owners, and others with security-significant responsibilities, were intimately familiar with the systems and operating environment. Therefore, he believed that the system security plans and supporting documents were sufficient. However, in addition to being contrary to Federal and Department direction, this practice could prove problematic should individuals that are unfamiliar with the environment need to review or implement the plans. For example, a third-party security assessor would not be familiar enough with the LLNL computing environment to design assessment procedures for a system without reliance on a well-defined system security plan and SPP document. In addition, an assessment conducted by the Department's Office of Health, Safety and Security in 2008 identified similar weaknesses with the site's security planning activities. To help address this issue, subsequent to our review, LSO officials stated that they had provided guidance to LLNL regarding the level of specificity required for security control descriptions.

The designated LSO Federal official also had not ensured that security-significant system changes were brought to his attention for review and approval. Although NNSA policy required that security-significant changes be determined by the Designated Approving Authority, site-level policy and procedures approved by the Federal Authorizing Official gave LLNL's cyber security organization full discretion to determine whether security-significant changes to national security

---

systems increased residual risk and thus should be presented to the designated Federal official. The Federal Authorizing Official's representative told us that having these changes approved by the cyber security organization was acceptable because that official was comfortable that the cyber security organization had enough familiarity with the systems. To his credit, the designated Federal official recently issued direction to the site outlining specific instances of system changes that required his explicit approval. In addition, the Federal Authorizing Official's representative noted that LSO performed broad assessments to determine whether the site contractor had met contract performance measures for security, which included limited reviews of security controls on national security information systems.

### **National Security Information Systems Assurance**

Without improvements, LLNL contractor and Federal officials may not be able to make informed risk-based decisions that support the protection of classified information and the systems on which it resides. For example, LLNL contractor officials did not test all Federally-required controls during recent system authorization activities due to their exclusion from program-level policy. As a result, the existence and need for implementation of those controls was not part of the site's risk-based consideration to operate the systems. In addition, incomplete descriptions of controls in system security plans may limit the ability of officials to test the effectiveness of controls over the information systems. Furthermore, system operators could potentially introduce untested, security-significant changes that may impact the risk to the LLNL computing environment if changes are made without the knowledge and approval of designated Federal officials. As noted in our *Special Inquiry Report to the Secretary: Selected Controls over Classified Information at the Los Alamos National Laboratory* ([OAS-SR-07-01](#), November 2006), numerous weaknesses in controls over national security information systems, including an inadequate change control process, contributed to the unauthorized release of classified information.

### **RECOMMENDATIONS**

To help improve the effectiveness of the risk management process for national security systems, we recommend that the Administrator, National Nuclear Security Administration, in conjunction with the NNSA Chief Information Officer:

- 
1. Revise the NNSA Policy Letters to more closely reflect current direction from the Department and the CNSS; and,
  2. Develop and implement effective procedures for monitoring the adequacy and sufficiency of protections over national security information systems.

We recommend that the Manager, Livermore Site Office, direct cognizant Lawrence Livermore National Security officials to:

3. Ensure that information system owners and system security officers employ a fully effective risk management process, to include ensuring that system security plans adequately address all minimum security controls; and,
4. Ensure that security-significant changes potentially impacting the risk to information systems are consistently elevated to the Federal Authorizing Official for explicit approval.

## **MANAGEMENT REACTION**

Management indicated that it generally agreed with the report's findings. While LSO did not agree with the report's recommendations, management commented that corrective actions were already underway to address weaknesses identified in the report. However, no specific corrective actions were included in management's comments. In addition, management disagreed with several of the conclusions in the report, as summarized below.

Management commented that it did not believe the conclusions documented in our report can be extrapolated to determine the state of the entire risk management program at LLNL. Rather, management stated that the findings in the report should only reflect issues surrounding the maintenance of security documentation and issues that LSO had self-identified as part of its performance monitoring process. In addition, management commented that it was not appropriate to measure LLNL against Federal requirements for security controls and system categorizations that were not included in its contract or NNSA policy. LSO believed that it was inappropriate to require LLNL to implement controls not authorized or funded by the Department and/or NNSA. Specifically, management stated that LLNL was not required to follow CNSS Instruction 1253, but noted that the Department was working to update its cyber security directive to include this Federal policy. LSO officials

---

also disclosed that the issues we identified with the site's performance monitoring activities were a result of direction received from NNSA Headquarters. Furthermore, management was concerned with changes to the scope of the audit and commented that the report should be modified to separate issues at NNSA Headquarters from those specific to LLNL. At the conclusion of our audit, NNSA officials commented that a contributing factor to the problems identified during our review was the Department's inability to update existing cyber security directives in a timely manner to meet Federal requirements. Officials believed that this impacted their ability to update program-level policies and resulted in certain security requirements not being met.

## AUDITOR COMMENTS

While we acknowledge management's concerns, we believe that the findings and recommendations identified in the report are appropriate. In particular, we agree that LLNL was not responsible for implementing baseline security controls that were not included in contractually required directives. However, as noted in our report, it was the responsibility of NNSA management to ensure that its policies were updated in a timely manner and implemented as appropriate. We also agree that LSO's performance monitoring activities were impacted when NNSA issued its moratorium on site assessments; and we modified our report to better reflect the reasons monitoring had not been performed.

Although management noted in its comments that the Department was updating DOE Order 205.1A to include CNSS Instruction 1253, such modifications remained incomplete. In addition, most of the issues identified in our report were related to not meeting existing Department and/or NNSA requirements, not CNSS Instruction 1253. Furthermore, while management was concerned about changes to the scope of the audit, we believe it was appropriate to limit our review to LLNL and Headquarters due to the issues identified at the site. Also, because a number of the weaknesses identified at LLNL were the result of inadequate policies issued by NNSA Headquarters, the inclusion of both Headquarters and site-specific issues in the report was appropriate. In addition, our evaluation focused on reviews of documentation maintained to support the site's risk management process as well as reviews of the processes used by the site to manage cyber security. We modified our report, as necessary, in response to management's comments.

Management's comments are included in Appendix 3.

## **Appendix 1**

---

<b>OBJECTIVE</b>	To determine whether the National Nuclear Security Administration (NNSA) had developed and implemented an effective risk management process over its national security information systems at the Lawrence Livermore National Laboratory (LLNL).
<b>SCOPE</b>	The audit was performed between March 2010 and April 2011, at Department of Energy (Department) Headquarters in Washington, DC and at the LLNL in Livermore, California. The audit was limited to a review of LLNL's risk management process for national security information systems, but did not include a review of systems containing Sensitive Compartmented Information.
<b>METHODOLOGY</b>	<p>To accomplish our objective, we:</p> <ul style="list-style-type: none"><li>• Reviewed applicable laws and Department directives, including those pertaining to security of national security information systems;</li><li>• Reviewed applicable standards and guidance issued by the Office of Management and Budget, the Committee on National Security Systems, and the National Institute of Standards and Technology;</li><li>• Reviewed prior reports issued by the Office of Inspector General and the Office of Health, Safety and Security;</li><li>• Obtained documentation from and held discussions with officials from the Department's Office of the Chief Information Officer, NNSA, and contractor personnel relating to system security; and,</li><li>• Analyzed system documentation to determine whether the risks of operating selected national security information systems had been addressed.</li></ul>

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal

## **Appendix 1 (continued)**

---

controls and NNSA's implementation of the *Government Performance and Results Act of 1993* and determined that it had established performance measures for cyber security reviews, but these were not necessarily specific to the management and operation of its national security information systems. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely on computer-processed data to satisfy our audit objectives. Our review also did not include technical testing of specific information systems.

An exit conference was held with NNSA officials on April 4, 2011.

## **Appendix 2**

---

### **RELATED REPORTS**

#### **Office of Inspector General Reports**

- *Certification and Accreditation of the Department's National Security Information Systems* ([DOE/IG-0800](#), August 2008). We found that at five of the six sites included in our audit, risks such as a lack of separation of duties and the presence of unclassified and classified systems operating in the same environment had not been addressed in system security plans. In many instances, security plans, or changes to systems, were not appropriately approved by Department of Energy (Department) officials. Further, in certain cases, plans did not accurately reflect the actual environment in which the system operated; and, at five of the six sites reviewed, contingency plans had not been developed for national security information systems – a critical activity required to mitigate the risk of service disruption. Several problems contributed to the weaknesses identified during our review. In particular, the Department had not yet fully developed and implemented adequate cyber security policies to ensure that national security information systems were adequately protected. In addition, Federal and contractor officials did not always utilize effective mechanisms to monitor performance of security controls.
- *Special Inquiry Report to the Secretary: Selected Controls over Classified Information at the Los Alamos National Laboratory* ([OAS-SR-07-01](#), November 2006). Our review revealed that significant and pervasive information security weaknesses placed Los Alamos National Laboratory's (LANL) classified computing operations and assets at high risk. We found that while LANL had developed policies designed to protect classified information, in many instances these were not effectively deployed to prevent serious security weaknesses at the classified computing facility. Specifically, classified information was diverted by a subcontract employee using an unapproved – but readily accessible – networked printer and an unauthorized flash drive to copy and remove classified information. In addition, we identified deficiencies related to mixed-media vulnerabilities, unneeded access to computing resources, as well as a failure to operate within classified information system accreditation boundaries.

## **Appendix 3**

---

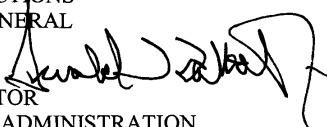


**Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585**

February 10, 2011



MEMORANDUM FOR: RICKEY R. HASS  
DEPUTY INSPECTOR GENERAL  
FOR AUDITS AND INSPECTIONS  
OFFICE OF INSPECTOR GENERAL

FROM: GERALD L. TALBOT, JR.   
ASSOCIATE ADMINISTRATOR  
FOR MANAGEMENT AND ADMINISTRATION

SUBJECT: NNSA's Comments to the IG's draft report on Livermore's National Security Information Systems, Project Number A10TG023; IDRMS No. 2011-00412

The National Nuclear Security Administration (NNSA) appreciates the opportunity to comment on the Inspector General's (IG) draft report, *Risk Management Process for National Security Information Systems at Lawrence Livermore National Laboratory*. I understand that the IG performed this audit to determine if the Department adequately protecting its classified computing information systems.

NNSA generally agrees with findings identified in the report; however, we disagree with several conclusions drawn as the IG did not complete the necessary actions to support those conclusions. The IG review was based on a paper-based compliance review assessing system level and some site level documentation. It appears there were inadequate discussions/review of mitigation strategies/activities implemented to address the constant changes addressing threats, vulnerabilities, technologies and mission/business processes of each system to include the current state of Departmental policies. We do not believe conclusions documented in this report can be extrapolated to determine the state of the entire Risk Management Program at the Site. The IG did not conduct a risk-based performance review to further validate conclusions based on physical assessment of the effectiveness of the controls implemented in the context of the risk profile of the Site. As such, the findings in this report should only reflect issues surrounding the maintenance of security documentation and the issues that the Livermore Site Office (LSO) had already self identified within its accreditation and certification process. Furthermore, the general recommendations made by the IG were already in place hence the corrective actions that are being performed at the Site and Department level.

With respect to the IG's second finding documented under the section titled Results of Audit, the IG inappropriately assessed the Lawrence Livermore National Laboratory's (LLNL) documentation against Committee on National Security Systems Instruction (CNSSI) 1253 "Security Categorization and Control Selection for National Security Systems" holding them accountable to implementing controls not authorized by the Department. Upon release of national standards such as 1253, Sites are to wait the direction of the Department via

 Printed with soy ink on recycled paper

## **Appendix 3 (continued)**

---

Departmental Policies as these changes require further direction on addressing the unique information processed, stored, maintained and owned by the Department and is not taken into consideration in national level standards. Attached are comments from LSO, which NNSA management agrees with, that the IG's results and recommendations as it relates to policy are based on inaccurate and incomplete review of Departmental Policies as these issues should be addressed at the Departmental level and not the site.

In conclusion, we do not concur with the outcome of this review as the initial scope was reduced from a review of all Sites (DOE-wide) to only one Site. We understand that it is the IG discretion to change the scope of a review; however, we believe that this descoping limits the Department's ability to compare this Site's performance in maintaining security documentation relative to others. Furthermore, IG revised the objectives of the review months after the start by incorporating national level standards which had not been approved nor funded by the Department.

If you have any questions concerning this response, please contact JoAnne Parker, Director, Office of Internal Controls at 202-586-1913.

Attachment

cc:      Robert Osborn, Chief Information Officer  
             Wayne Jones, Deputy Chief Information Officer  
             Alice Williams, Manager, Livermore Site Office

## 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 Felicia Jones at (202) 586-7013.

This page intentionally left blank.

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.