



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

# Inspection Report

---

Reporting of Security Incidents  
at the Lawrence Livermore National  
Laboratory

DOE/IG-0625

November 2003



## Department of Energy

Washington, DC 20585

November 4, 2003

### MEMORANDUM FOR THE SECRETARY

FROM: *Greg Friedman*  
Gregory H. Friedman  
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Reporting of Security Incidents at the Lawrence Livermore National Laboratory"

### BACKGROUND

The Department of Energy's (DOE) Lawrence Livermore National Laboratory (Livermore) performs research and development activities that require the highest levels of security. On May 5, 2003, Livermore officials reported to DOE that a set of master keys had been discovered missing on April 17, 2003. On May 30, 2003, Livermore officials reported to DOE that a master Tesa card, which is a plastic card-like key with a magnetic strip, had been discovered missing on April 12, 2003. The loss of the master keys and Tesa card, and the delay in reporting these losses, raised the possibility of security vulnerabilities at the Laboratory. The purpose of this inspection was to determine the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as missing master keys and master Tesa cards, and the identification and correction of corresponding potential security vulnerabilities.

### RESULTS OF INSPECTION

We concluded that Livermore did not have adequate internal controls to ensure that: (1) security incidents involving missing master keys and Tesa cards were reported within required timeframes, and (2) that timely follow-up actions were taken to identify and address any potential security vulnerabilities resulting from the incidents. Specifically, we found that Livermore security officials:

- Misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card;
- Did not report the security incidents involving the missing master keys and master Tesa card to DOE within required timeframes;
- Did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card; and



- Did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

During our review we learned that during a May 2003 inventory, Livermore officials identified an additional three master keys and two master Tesa cards that were missing. Although two of the three master keys had been reported missing by the Livermore Fire Department to the Protective Force Division more than three years before, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. Recent DOE and Livermore oversight reviews of Livermore's safeguard and security operations did not identify internal control weaknesses related to the control and inventory of master keys and master Tesa cards.

As a result of the potential security vulnerabilities caused by the missing master keys, Livermore eventually initiated actions to replace or upgrade locks at significant cost. Livermore officials initially estimated the cost to replace or upgrade the locks as \$1.7 million. This figure was challenged upon release of our draft report. However, as of the date of this report, officials of the National Nuclear Security Administration (NNSA) have not provided a different cost figure. Ultimately, Federal taxpayers will bear this cost. We believe that Livermore failed to ensure compliance with established internal controls over the master keys and master Tesa cards, and as such, we question the allowability of these costs.

#### MANAGEMENT REACTION

Management did not specifically state concurrence with our recommendations. However, management identified corrective actions that NNSA believes are responsive to our recommendations. These actions include implementing additional procedures and training.

Although this is a good first step, management needs to do more to assure that Livermore places greater emphasis on the need to strictly follow its processes and procedures for accountability and control of security keys. Management stated that such processes are captured in site security surveys and self-assessments, but acknowledged that they were not followed in these cases. Similarly, an October 14, 2003, press article reported that a gate to a limited security area at the Laboratory, a secured facility, was left unlocked. In our view, this latest incident only serves to reinforce the need for greater commitment by Laboratory management and personnel to prevent security incidents, and when they occur, to report and resolve them promptly.

Attachment

cc: Deputy Secretary  
Administrator, National Nuclear Security Administration  
Under Secretary for Energy, Science and Environment  
Manager, Livermore Site Office  
Director, Policy and Internal Controls Management

# REPORTING OF SECURITY INCIDENTS AT THE LAWRENCE LIVERMORE NATIONAL LABORATORY

---

## TABLE OF CONTENTS

### **OVERVIEW**

Introduction and Objectives .....	1
Observations and Conclusions .....	2

### **DETAILS OF FINDINGS** .....

4

Reporting Thresholds for Security Incidents .....	4
Reporting Security Incidents to DOE/NNSA .....	5
Additional Missing Keys .....	6
Security Risk Assessments .....	7
Compensatory Measures .....	7
Performance Measures .....	9
Oversight Reviews .....	9

### **RECOMMENDATIONS** .....

10

### **MANAGEMENT COMMENTS** .....

11

### **INSPECTOR COMMENTS** .....

12

### **APPENDICES**

A. Scope and Methodology .....	13
B. Management Comments .....	14

# Overview

---

## INTRODUCTION AND OBJECTIVES

Lawrence Livermore National Laboratory (Livermore) performs research and development activities in support of national defense that require the highest levels of security. The University of California (UC) manages and operates Livermore under contract with the Department of Energy (DOE), which includes the National Nuclear Security Administration (NNSA).

On May 13, 2003, Livermore officials issued a Press Release stating that a set of master keys assigned to a Livermore Protective Force Officer had been discovered missing on April 17, 2003. Later, on May 30, 2003, a Livermore official announced to employees that a master Tesa card, which is a plastic card-like key with a magnetic strip, had been discovered missing on April 12, 2003.

Keys and electronic entry cards are an essential component of the system of access controls at Livermore and other DOE sites. Unique keys and cards, by their nature, serve to restrict access by unauthorized individuals to specific areas that may contain classified information and materials, sensitive program, project or proprietary information, or the personal belongings of Laboratory employees. Master keys and cards, on the other hand, control access to a significant number of the facilities, buildings and offices at Livermore. Their distribution is restricted to a limited number of personnel in order to ensure the integrity of the unique key and card access control component.

The objectives of this inspection were to determine: (1) the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as the missing master keys and master Tesa cards, and the identification and correction of corresponding potential security vulnerabilities; and (2) if performance measures exist at Livermore that adequately address the reporting of such incidents.

---

**OBSERVATIONS AND CONCLUSIONS**

We concluded that Livermore did not have adequate internal controls to ensure that security incidents involving missing master keys and master Tesa cards were reported within required timeframes, and that timely follow-up actions were taken to identify and address potential security vulnerabilities resulting from the incidents.

Specifically, we found that Livermore security officials:

- Misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card;
- Did not report the security incidents involving the missing master keys and master Tesa card to DOE/NNSA within required timeframes;
- Did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card; and
- Did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

During our review we learned that Livermore officials initiated a complete inventory in May 2003, to determine the status of all master keys and master Tesa cards at Livermore. The inventory disclosed that an additional three master keys and two master Tesa cards were missing. This brought the total number of missing master keys to nine, and the total number of missing master Tesa cards to three. Two of the three missing master keys were from a set of keys that the Livermore Protective Force Division set aside for use by the Livermore Fire Department. A Fire Department official told us that the two master keys had been reported missing to the Protective Force Division over three years ago. However, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. We were told that at that time, the view of the Protective Force Division was that the set of keys contained fewer master keys than were typically found on other sets of keys, not that any master keys were missing.

---

Although keys and cards are only one component of the system of access controls at Livermore, the loss of the master keys and master Tesa cards affected the level of security afforded classified and sensitive areas at Livermore. As a result of the potential security vulnerabilities caused by the missing master keys, Livermore eventually initiated actions to replace or upgrade locks at significant cost. We were initially advised by Livermore officials that the estimated cost to replace or upgrade the locks was \$1.7 million. Commenting on our draft report, NNSA officials did not believe the cost estimate was consistent with the Laboratory's expenditures or numbers of locks to be replaced. However, as of the date of this report, NNSA officials had not provided a revised cost figure. Ultimately, Federal taxpayers will bear this cost. We believe that Livermore failed to ensure compliance with established internal controls over the master keys and master Tesa cards. Therefore, we question the allowability of these costs.

## Details of Findings

---

### **REPORTING THRESHOLDS FOR SECURITY INCIDENTS**

We found that Livermore security officials misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card.

### **Reporting Requirements**

DOE Notice 471.3, "Reporting Incidents of Security Concern," establishes four reporting thresholds for incidents of a security concern under an Impact Measurement Index (IMI) system. The highest reporting threshold, IMI-1, is for "Any security incident that can be expected to cause serious damage to national security or DOE security interests." The lowest reporting threshold, IMI-4, is for "Any security incident that causes no damage to national security, but that can, in combination, indicate weakened security awareness or inadequate procedures or practices."

At Livermore, the Safeguards and Security Department's Office of Incidents and Infractions is the responsible entity for reporting security incidents to DOE in accordance with DOE Notice 471.3. This office relies, in part, on the Protective Force Division providing reports on individual incidents that have occurred at Livermore so that a reporting determination under DOE Notice 471.3 can be made.

A Livermore security official informed us that on two occasions immediately following the loss of the set of master keys on April 17, 2003, a review was conducted of the security incident reporting criteria. According to the official, the reviews did not identify a need to report the loss of the master keys to DOE. The official said that another Livermore security employee discussed the loss of the keys with Livermore's Office of Incidents and Infractions and was told by that office that the loss of the master keys did not require reporting to DOE. According to an employee in the Office of Incidents and Infractions, his review of the IMI reporting categories in the DOE Notice did not identify a specific reference to "missing master keys," but it was unclear in his mind whether or not the loss of the keys was reportable.

The loss of a master Tesa card on April 12, 2003, was not reviewed by the Office of Incidents and Infractions for reporting under DOE Notice 471.3 until the office received an Incident Report from the Protective Force Division on or about May 30, 2003. The loss of the master Tesa card was reported at that time as an IMI-4 incident.



---

## Security Implications

Although the set of master keys and the master Tesa card opened locks leading to some of the most sensitive areas of the Laboratory, Protective Force Division officials did not perceive the loss as having the potential to cause damage to national security or DOE security interests. A Protective Force Division official advised us that they had lost keys before and that the keys had always turned up. The official told us that when the set of master keys did not turn up after a few days of extensive searching, the Protective Force Division became involved in other security issues and did not focus on the security implications of the missing keys. In addition, the official stated that the Protective Force Division was not aware that during the period that the master keys were missing, a master Tesa card was also missing. The Protective Force Division did not consider the security implications of the double failure<sup>1</sup> resulting from the two types of master keys (i.e., keys and Tesa card) being missing at the same time.

After Livermore senior management became aware of the missing master keys on May 5, 2003, the Office of Incidents and Infractions classified the incident at the lowest reporting threshold, IMI-4, that is, a security incident “that causes no damage to national security.” It was not until the intervention of a senior NNSA official on May 9, 2003, that the Office of Incidents and Infractions re-evaluated the incident and reclassified it as an IMI-2, which is defined as “Any security incident that can be expected to cause damage to national security or DOE security interests.”

## REPORTING SECURITY INCIDENTS TO DOE/NNSA

We found that Livermore security officials did not report the security incidents involving the missing master keys and master Tesa card to DOE/NNSA within required timeframes.

## DOE Notice

DOE Notice 471.3 states that a facility has 24 hours to determine if a security incident should be reported. If the incident should be reported, it must be categorized under the IMI system. The most serious category of security incidents, IMI-1, must be reported to DOE within one hour after categorization; IMI-2 and IMI-3 incidents must be reported within 8 hours; and summaries of IMI-4 incidents are to be reported monthly.

However, these incidents were not reported to DOE/NNSA until weeks after they were first recognized. Specifically:

- The master Tesa card discovered missing on April 12, 2003, was not reported to DOE/NNSA until May 30, 2003.

---

<sup>1</sup> A double failure occurs when the two primary types of security locks protecting the same area are compromised at the same time.

- 
- The set of six master keys discovered missing on April 17, 2003, was not reported to DOE/NNSA until May 5, 2003.

We learned that Protective Force Division officials had no immediate plans of reporting the missing keys to Livermore management or DOE. A Protective Force Division official advised us that the issue of the missing keys was on a list of things to discuss with higher management, but the issue was never discussed. The missing keys went unreported until May 5, 2003, when an alert employee in the Livermore Locks and Keys Shop became aware of an attempt by the Protective Force Division to have a duplicate set of the master keys made to replace the missing set, and promptly alerted security officials in the Safeguards and Security Department of the missing master keys.

Similarly, the missing master Tesa card went unreported until May 30, 2003. Although the Protective Force Division Incident Report was dated April 12, 2003, the Office of Incidents and Infractions did not receive the report until an employee in the Safety, Security and Environmental Protection Directorate alerted senior Livermore management about the missing master Tesa card.

## **ADDITIONAL MISSING KEYS**

We found that Livermore security officials could not determine how long other master keys and master Tesa cards had been missing.

In May 2003, Livermore security officials initiated a complete inventory to determine the status of all master keys and master Tesa cards. The inventory disclosed that an additional three master keys and two master Tesa cards were missing. Two of the three missing master keys were on a set of keys used by the Livermore Fire Department. A Fire Department official told us that the two master keys had been reported missing to the Protective Force Division over three years ago. However, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. At that time, the view of the Protective Force Division was that the set of keys contained fewer master keys than were typically found on other sets of keys, not that any master keys were missing.

The two missing master Tesa cards had been placed in storage by the Protective Force Division. The Protective Force Division could not locate the two master Tesa cards during the inventory.

Livermore security officials were unable to ascertain when the master keys and master Tesa cards were lost. Based on our review, we concluded that Livermore did not have adequate inventory

---

controls over its master keys and master Tesa cards. We consider such controls to be a fundamental part of the security regime at an institution like Livermore that is responsible for conducting highly classified and sensitive activities in support of national defense. Upon completion of the May 2003 inventory, Livermore officials notified DOE/NNSA of the additional missing master keys and master Tesa cards.

## **SECURITY RISK ASSESSMENTS**

We found that Livermore security officials did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card.

The master keys were missing for over two weeks before any consideration was given to assessing potential security risks to identify possible vulnerabilities. On May 6, 2003, a Safeguards and Security Department official directed that a risk assessment be conducted, which included the most sensitive areas of the Laboratory. A Livermore Safeguards and Security Department official then directed the conduct of a second risk assessment that included national security assets such as classified matter, unclassified controlled nuclear information, high explosives, biological assets, Category IV Special Nuclear Material (SNM) and firearms.

The master Tesa card was missing for 32 days before a notification was made to Livermore program officials. On May 14, 2003, Safeguards and Security Department officials informed Laboratory program officials of the loss and the need for assessing potential security risks. During this meeting the security implications of the double failure were discussed for the first time, one month after the double failure condition occurred.

## **COMPENSATORY MEASURES**

We found that Livermore security officials did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

Protective Force Division officials took no compensatory measures to address potential security vulnerabilities associated with the missing master keys and master Tesa card prior to May 6, 2003. A Protective Force Division official advised us that they were not aware of the double failure resulting from the combination of the missing master keys and master Tesa card until a meeting in early May 2003. However, the official said that compensatory measures should have been taken with respect to the missing master keys anyway. According to the official, the focus at the time was on finding the keys, and that when the keys were not found, their

---

focus changed to other protective force issues and they did not address the issue of compensatory measures.

Short-term compensatory measures, which were the result of intervention by Livermore management outside the Protective Force Division, were not initiated until May 6, 2003. These measures, which consisted of block-out blades, door seals, re-keying, suspension of the day-lock-rule<sup>2</sup>, and installation of additional Tesa locks, were completed a month or more after the master keys and master Tesa card were discovered missing.

The dates of discovery of the respective missing master keys and master Tesa cards and the dates they were reported to DOE/NNSA as missing are shown in Figure 1.

#### **Summary of Missing Master Keys and Tesa Cards**

<b>Type of Key</b>	<b>Date Missing</b>	<b>Date Reported</b>
1 Master Tesa	April 12, 2003	May 30, 2003
6 Master Keys	April 17, 2003	May 5, 2003
2 Master Keys	3 or more years <sup>3</sup>	May 30, 2003
1 Master Key	Indeterminate Period	May 31, 2003
2 Master Tesa	Indeterminate Period	June 2, 2003

**Figure 1**

#### **Corrective Action Plans**

We were advised by an NNSA official that on June 12, 2003, the NNSA Livermore Site Office issued three major findings to Livermore related to security locks and keys. We were also advised that by July 2003, formal corrective action plans to correct vulnerabilities in security incident reporting and security key control and inventory procedures were in place. According to the NNSA official, Livermore has completed several corrective action plan milestones, which will be validated by the Livermore Site Office by the end of December 2003.

---

<sup>2</sup> The day-lock-rule allows classified materials to be left unattended for brief periods provided that other security measures (i.e. items secured in a locked room) are in place to prevent unauthorized access.

<sup>3</sup> Keys reported by the Livermore Fire Department as missing more than three years ago.

---

**Cost of Lock Replacement**

With reliance on a complex lock, key, and Tesa card security strategy at Livermore to prevent access to classified and sensitive areas, there is little doubt that the level of security afforded these areas was adversely affected. Livermore officials initially advised us that, in the long-term, the loss of the master keys would require the replacement and upgrade of approximately 100,000 locks in both classified and unclassified areas within 526 buildings. They also initially estimated the total cost of this lock replacement project, which also includes upgrading existing locks, at approximately \$1.7 million. However, as of the date of this report, NNSA officials had not validated this figure as accurate.

UC is required by Clause I.062 of its contract with DOE to have methods and procedures in place to reasonably ensure that the mission and functions assigned to the contractor are efficiently and properly executed, and that resources are safeguarded against waste, loss, and mismanagement. As reported by an internal Livermore review team, Livermore violated its internal control procedures for the control and accountability of master keys. This resulted in the need to replace and upgrade locks, and take other compensatory measures. We were told that prior to the loss of the master keys in April 2003, no such lock replacement project had been planned. Based on Livermore's failure to exercise due diligence in performing its contractual responsibilities, we question whether these costs are allowable.

**PERFORMANCE MEASURES**

Our review of the contractor performance self-assessment criteria for Fiscal Year 2003 revealed that a specific statement to "Conduct analysis of [the] incident pertaining to key control and accountability" was added to the Livermore Safeguards and Security Assessment Management Plan in June 2003. We were told by a senior NNSA Livermore Site Office official that a Livermore self-assessment performance review of the results of Fiscal Year 2003 Safeguards and Security operations will be conducted and that it will include the missing key incidents detailed in this report.

**OVERSIGHT REVIEWS**

Recent DOE and Livermore oversight reviews of Livermore's safeguards and security operations prior to the disclosure of the missing master keys and missing master Tesa card, did not identify internal control weaknesses related to the control and inventory of master keys and master Tesa cards. Guides developed by various organizations to plan and conduct these reviews suggest that processes should be reviewed to determine whether procedures are in place to adequately control keys and locks. However, none of these oversight reviews identified the key control and inventory weaknesses at

---

Livermore that allowed master keys and Tesa cards to go missing for an extended period of time without detection.

Several security surveys and self-assessments performed by NNSA and Livermore since 2000 did not report any issues relating to key control and inventories. These reviews consistently rated topical areas that included key control and inventories as “satisfactory.” Although a 2003 security survey verified the existence of lock and key records and procedures, the survey did not evaluate the accuracy or effectiveness of the records and procedures in controlling and accounting for keys.

In comments to our draft report, the NNSA Associate Administrator for Management and Administration stated that although NNSA believes the processes in place related to the security of keys are captured in the surveys and self-assessments, the established processes and procedures were not followed. He stated that NNSA will provide a copy of our recommendations and NNSA’s expectations to the Site Office Managers for their inclusion in their respective oversight processes.

We believe that future field site security surveys and self-assessments should include a review of internal controls relating to the issuance, receipt, and inventory of keys that provide access to sensitive areas.

We noted that a 2002 DOE assessment of physical security systems at Livermore included a review of barriers protecting special nuclear material facilities. The missing master keys and Tesa cards accessed locks in some of these facilities. The assessment report was silent regarding whether master keys and Tesa cards were included in the review. However, Livermore physical security systems received a rating of “EFFECTIVE PERFORMANCE.”

## **RECOMMENDATIONS**

We recommend that the Administrator, National Nuclear Security Administration:

1. Ensure that field site security surveys and self-assessments include a review of internal controls relating to the issuance, receipt, and inventory of all keys involving sensitive areas.

We also recommend that the Manager, Livermore Site Office:

2. Review the costs incurred by Livermore to replace and upgrade approximately 100,000 locks necessitated by the missing master keys and master Tesa cards, to determine whether the costs are reasonable and allowable.

- 
3. Ensure that Livermore establishes appropriate internal controls to correctly identify reportable incidents, and that such incidents are reported in a timely manner.
  4. Ensure that Livermore officials responsible for categorizing incidents reportable under DOE Notice 471.3 are trained to properly determine the appropriate IMI classification level of security incidents.
  5. Ensure that internal controls are established by Livermore that promote the timely assessment of vulnerabilities resulting from security incidents, and the prompt implementation of compensatory measures.
  6. Ensure that Livermore has established appropriate internal controls for the management and inventory of master keys and master Tesa cards.

## **MANAGEMENT COMMENTS**

In comments to our draft report, the NNSA Associate Administrator for Management and Administration stated that the report is consistent with the findings of Laboratory, Livermore Site Office, University of California and NNSA reviews of the security locks and keys incidents. While the Associate Administrator did not specifically state concurrence with our recommendations, he identified corrective actions taken by the Livermore Site Office and the Laboratory that he believed were responsive to our recommendations.

Regarding recommendation 1, the Associate Administrator acknowledged that while processes related to security of keys are captured in surveys and self-assessments, the established policies and procedures were not being followed. He stated that NNSA will provide a copy of our recommendations and NNSA's expectations to the Site Office Managers for their inclusion in their respective oversight processes.

Regarding recommendation 2, the Associate Administrator stated that the contracting officer already determined that the costs incurred to change the locks are allowable and reasonable under the terms of the contract, and NNSA did not believe that the matter requires an "Allowability of Cost Determination." However, he advised that NNSA is requesting a General Counsel opinion as to what warrants an "Allowability of Cost Determination." In addition, the Associate Administrator did not believe the \$1.7 million figure stated in our draft report to replace or upgrade

---

approximately 100,000 locks was consistent with the Laboratory's expenditures or number of locks being replaced. The Associate Administrator did not provide figures for the actual cost and numbers of locks to be replaced. In addition, as of the date of this report, NNSA has not provided these figures.

Regarding recommendations 3, 4, 5, and 6, the Associate Administrator identified ongoing and completed corrective actions taken by the Livermore Site Office and Laboratory management that he felt were responsive to our recommendations.

The complete text of management's comments are attached at Appendix B.

## **INSPECTOR COMMENTS**

Management's actions appear responsive to the report recommendations. However, we do not agree that the total cost of replacing and upgrading the locks are "part of the normal cost of doing business." Livermore did not follow its internal procedures for the control and accountability of master keys and master Tesa cards, which created a security vulnerability that resulted in the need to replace and upgrade a significant number of locks. By not complying with its contractual responsibilities, the Laboratory unnecessarily incurred a substantial cost that we believe is unallowable and should not be borne by the taxpayer.

Management identified actions implemented by the Livermore Site Office and the Laboratory to ensure proper reporting of incidents such as the missing master keys and master Tesa cards. These actions included implementation of additional procedures and training. We believe these actions are a good first step to address the problems discussed in our report. However, as acknowledged by the Associate Administrator, in specific instances established processes and procedures were not followed. Therefore, in addition to issuing additional procedures, we believe management should assure that a culture exists wherein individuals will fully implement the procedures.



## Appendix A

---

### SCOPE AND METHODOLOGY

The fieldwork for this inspection was conducted between May and July 2003. We interviewed numerous Livermore and NNSA Livermore Site Office officials regarding their knowledge of the missing master keys and master Tesa cards. We also reviewed available documentation from the Livermore internal and external review teams that evaluated the missing master key and master Tesa card incidents. The documentation that we reviewed included:

- Incident Assessment Team Report: Key Incident of April 17, 2003.
- Independent External Review Team “Report on the Lawrence Livermore National Laboratory Security Key Incident.”
- Incident Analysis Team Report dated May 30, 2003.
- Master Tesa Inventory Process Report (Revision 1), dated June 6, 2003.
- Lawrence Livermore National Laboratory “Locks and Keys Guide.”
- Fiscal Year 2003 Appendix F, Performance Assessment Mid-Year Review.
- Integrated Safeguards and Security Management Project Plan, dated December 14, 2001.
- LLNL Implementation Guidelines for Fiscal Year 2003 Appendix F Performance Objectives and Measures.

We also reviewed the contract between DOE and the University of California for the management and operation of Lawrence Livermore National Laboratory, as well as:

- DOE Notice 471.3, “Reporting Incidents of Security Concern.”
- DOE Notice 473.8, “Security Conditions.”

This inspection was conducted in accordance with the “Quality Standards for Inspections” issued by the President’s Council on Integrity and Efficiency.

# Appendix B

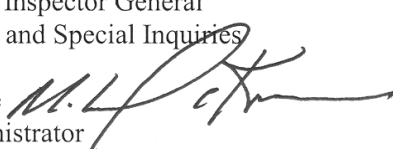


Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585



OCT 10 2003

MEMORANDUM FOR Alfred K. Walter  
Acting Assistant Inspector General  
for Inspections and Special Inquiries

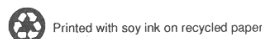
FROM: Michael C. Kane   
Associate Administrator  
for Management and Administration

SUBJECT: Comments to Draft Report on LLNL Security  
Incidents

NNSA appreciates the opportunity to review the Inspector General's (IG) draft Inspection report, "Reporting of Security Incidents at the Lawrence Livermore National Laboratory." We understand that the objectives of the inspection were to determine: (1) the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as the missing master keys and master TESA cards, and the identification and correction of corresponding potential security vulnerabilities; and, (2) if performance measures exist at Livermore that adequately address the reporting of such incidents.

We appreciate the IG's efforts and believe that the report is consistent with the findings of the Laboratory, Livermore Site Office, University of California, and NNSA conducted reviews of the security locks and keys incidents. While the report only explores the chronology and activities of the missing master keys and master TESA cards, NNSA believes that the report should acknowledge that formal corrective action plans, to correct vulnerabilities in security incident reporting and security key control and inventory, were prepared by the Laboratory, approved by the Site Office, and were already in place in July 2003. In fact, there were three major findings related to security locks and keys issued by the Site Office to the Laboratory on June 12. The Laboratory subsequently submitted the corrective action plans, with a detailed project schedule, for each of the findings to the Site Office. We believe it is important to mention that there are several corrective action milestones that have been achieved and will have been validated by the Site Office by the end of December.

The report has a recommendation related to the determination as to whether the costs associated with the corrective actions are reasonable and allowable. NNSA's position is that the costs are reasonable and allowable. However, we



---

realize the intent of the recommendation and by copy of this response, NNSA is requesting a General Counsel opinion as to what warrants an “Allowability of Cost Determination.” An “Allowability of Cost Determination” is a formal contract process utilized by Contracting Officers when there are questionable costs associated with a contract. We do not believe that this issue falls into that category. However, as stated, we look forward to the opinion of our General Counsel.

NNSA’s specific comments related to the recommendations are as follows:

1. For the Administrator to “Ensure that field site security surveys and self-assessments include a review of internal controls relating to the issuance, receipt, and inventory of all keys involving sensitive areas.”

NNSA believes that the processes are in place related to security of keys and are captured in the surveys and self-assessments. We further believe the established processes and procedures were not followed. NNSA will provide a copy of the recommendations and NNSA’s expectations to the Site Office Managers for their inclusion into their respective oversight processes.

2. Review the costs incurred by Livermore to replace and upgrade approximately 100,000 locks necessitated by the missing master keys and master TESA cards, to determine whether the costs are reasonable and allowable.

While NNSA does not believe that this issue requires an “Allowability of Cost Determination,” the contracting officer already determined that the costs incurred to change locks are allowable and reasonable under the terms of the contract. When keys are discovered missing that can create a potentially adverse security situation, it is incumbent upon the Laboratory to take appropriate action.

The \$1.7 million stated in the report to replace or upgrade approximately 100,000 locks is not consistent with the Laboratory’s expenditures or the number of locks being replaced. The resources committed to the corrective actions have come from existing program funding and include equipment upgrades made at the request of LLNL Programs. Installation of TESA electronic locks to replace mechanical keys/cores offers better modernized security and has been an ongoing process over the past five years. Replacing missing keys and TESA locks are considered part of the normal cost of doing business.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

3. Ensure that Livermore establishes appropriate internal controls to correctly identify reportable incidents, and that such incidents are reported in a timely manner.

Incident reports are distributed daily to appropriate personnel via fax to the Incidents and Infractions Section, Office of Investigative Services (OIS), Physical Security Group, and to the Site Office. The Laboratory has put in place procedures for classification review, risk assessment and dissemination of Protective Force Division (PFD) incident reports. Procedural documents: "LLNL Implementation Procedures for Reporting Incidents of Security Concern"; "Security Duty Officer Reporting Procedures"; "PFD Incident Report Review"; and, "Reporting Incidents of Security Concern" were submitted to the Site Office on September 30.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

4. Ensure that Livermore officials responsible for categorizing incidents reportable under DOE Notice 471.3 are trained to properly determine the appropriate IMI classification level of security incidents.

The Security Incident Reporting Officer and the Safeguards and Security Deputy Manager have received updated training provided by DOE/NNSA Headquarters in August.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

5. Ensure that internal controls are established by Livermore that promote the timely assessment of vulnerabilities resulting from security incidents and the prompt implementation of compensatory measures.

The Laboratory implemented and submitted a procedural document titled, "Security Duty Officer Reporting Procedures" on September 30, to the Site Office, to address vulnerabilities and implementation of compensatory measures.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

6. Ensure that Livermore has established appropriate internal controls for the management and inventory of master keys and master TESA cards.

---

The Laboratory has completed a 100 percent inventory and reconciliation of all grand master keys. Results of the inventory are written in a report titled, "Status of Master Security and 'Z' Key Inventory Process" dated July 25, 2003. Additionally, accountability and inventory requirements are written in each of the following documents: "Locks and Keys Policy" dated September 17, 2003; "Locks and Keys User Manual", dated September 30, 2003; and, "Locks and Keys Procedures" dated September 30, 2003.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

cc: NNSA General Counsel, NA-3.1  
Edward J. Knuckles, Assistant Manager-Business, Livermore Site Office  
Robert Braden, Senior Procurement Executive, NA-63  
David Marks, Field CFO, SvcCen/NV

## 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 Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page  
<http://www.ig.doe.gov>

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