



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

April 22, 2009

OFFICE OF THE ADMINISTRATOR

The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Congressman Barton:

This is in response to your March 27, 2009, letter regarding the Los Alamos National Laboratory's (LANL) January 2009 security incident, in which three government computers were stolen from an employee's home.

The enclosure addresses your questions regarding the steps taken by LANL management in efforts to improve the gaps in cyber security monitoring and oversight to prevent any future incidents.

If you have any additional questions or concerns, please contact me or James B. Lambert, Director, Office of Congressional, Intergovernmental and Public Affairs at (202) 586-7332.

Sincerely,

A handwritten signature in black ink that reads "T. P. D'Agostino". The signature is written in a cursive style.

Thomas P. D'Agostino
Administrator

Enclosure



CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 1 a.

What were the lost property protocols followed by Los Alamos National Laboratory management, Los Alamos National Security, LLS (LANS), during the time of the computer thefts cited in this letter?

A 1 a.

During the time of the computer theft, Los Alamos National Laboratory responded in accordance with the requirements outlined in site's property management manual. The manual requires employees to immediately report any lost, missing, stolen, vandalized, destroyed, or damaged Laboratory property to their supervisor, Property Administrator and EA-DO (Ethics and Audits, 5-3104) as soon as possible within 24 hours of the incident; use the Missing Item Checklist, found on the Laboratory EIA on-line forms website; and attach to the Missing Item Checklist, documentation related to the occurrence, such as police report.

Q 1 b.

How long had the lost property protocols been in place?

A 1 b.

The lost property protocols have been in place in excess of five years.

Q 1 c.

What deficiencies did the National Nuclear Security Administration identify?

A 1 c.

The following deficiencies were identified during the lesson learned session conducted by NNSA physical and cyber security personnel:

- Communication gap between the property management, information technology and cyber security division within the laboratory.
- Incident reporting gap between National Nuclear Security Administration and Los Alamos National Laboratory reporting process.

- Personnel understanding of the treatment of computer equipment during the incident reporting process (i.e. property and data).

While these were several deficiencies noted by NNSA HQ personnel during the lesson learned session, it is also important to note that LANL followed all of the current policies and procedures related to lost/stolen/missing equipment as outlined in their current M&O contract.

LANL/LASO POC:

Date:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 2 a.

Had the National Nuclear Security Administration previously evaluated these protocols?

A 2 a.

Yes

Q 2 b.

If no, why not?

A 2 b.

NA

Q 2 c.

If yes, what did the National Nuclear Security Administration determine?

A 2 c.

In July 2008, the NNSA Service Center conducted a review of the property management protocols at LANL. During this review it was sited that LANL was conducting business related to lost, damaged, destroyed, or stolen property as required by the current policy.

LANL/LASO POC:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 3.

What directives did the National Nuclear Security Administration site office issue?

Please provide any memoranda related to these directives, including, but not limited to, the NNSA Chief Information Officer memorandum dated January 27, 2009.

A 3.

1. January 26, 2009 memorandum from Russell Kirkpatrick (LASO SM) to Paul Sowa (LANL AD Safeguards and Security) subject "Missing/Stolen Computer Issue" requiring LANL to formalize notification procedures to include notifying LASO Cyber Security.
2. February 3, 2009 memorandum from Don Winchell (LASO Site Manger) to Michael Anastasio (LANL Director) and Rueben M. Rafferty (LANL Prime Contract Office), subject "Cyber Security / Property Management Concern" directing LANL to treat any loss of computer equipment with the capability to store data as a cyber security concern with reporting due to this office as outlined in the NNSA CIO's memorandum dated January 27, 2009.
3. In addition, the following memorandum was issued by NNSA Headquarters OCIO: January 27, 2009 memorandum from Linda Wilbanks (NNSA OCIO) to NA-1, Site Office Managers, Site Office DAAs, Site CIOs, subject "Computer Loss/Theft Reporting Requirements" mandating the loss or theft of any piece of equipment that has the capability to store information to be reported to the Department's Cyber Incident Response Capability within 24 hours.
4. NNSA Policy Letters (NAPs) - Cyber Security "B" Series issued September 27, 2006 and "C" Series Issued May 2, 2008. These policy letters implement requirements in Federal Law, Presidential Directives, Executive Orders, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Departmental policies while establishing cyber security processes that address program requirements, defining protection measures, and providing cyber security planning.

LANL/LASO POC:
HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:
Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

memorandum

National Nuclear Security Administration
Los Alamos Site Office
Los Alamos, New Mexico 87544

DATE: January 26, 2009
REPLY TO:
ATTN OF: SM: RKK (002-09)
SUBJECT: Missing/Stolen Computer Issue

TO: Paul Sowa, Associate Director, Safeguards & Security, LANL, MS-G729

Reference:

1. Contract Number DE-AC52-06NA25396, Los Alamos National Security, LLC and the Department of Energy, National Nuclear Security Administration
2. DOE M 470.4-1, Change 1

The Los Alamos Site Office (LASO) was informed by the Department of Energy (DOE)/National Nuclear Security Administration (NNSA) Headquarters this weekend of several Los Alamos National Security (LANS) owned computers being stolen from a LANS employee's home recently. The information was obtained for the Los Alamos Monitor and the Santa New Fe Mexican newspapers. LASO was notified by LANS of the incidents on January 20, 2009. There seems to be indications of the need to review reporting requirements and LANS property control measures and procedures.

Please provide the following information to LASO for response to the Office of the Chief, Defense Nuclear Security.

- Regarding the theft from the employee's home in Santa Fe, when was LANS notified of the theft and when was LASO notified of the theft?
- What is the level of information contained on each computer (OUO, UCNI, PII, etc.)?
- What is the status of the case and which department is investigating?
- Were all three government computers issued in compliance with LANS Policies and procedures for use at the employee's home?
- Number of recovered stolen LANS owned computers by law enforcement agencies in the past year and status of cases and names of involved agencies.
- Have the computers been examined forensically to see what level of information was on the computers?
- Number of computers stolen from LANS in the past year.
- Dates of notification to LANS and LASO of the thefts.
- Number of computers reported as missing and what is being done to locate them.
- LANL policy on justification and authorization for allowing employees to have government computing equipment off-site or at home.
- LANL policies and procedures for notifying LASO of thefts, loss and incidents involving government or LANS owned computers.

LASO and LANS need to formalize notification procedures to include notifying LASO Cyber Security.

Please respond to this request within 10 days of receipt of this memo to facilitate the LASO response to DOE/NNSA Headquarters and the Office of Defense Nuclear Security.

If the Contractor believes the Performance Direction violates Contract No. DE-AC52-06NA25396 Clause H-2 entitled Performance Direction; the Contractor shall suspend implementation of the Performance Direction and promptly notify the Contracting Officer of its reasons for believing that the Performance Direction violates this clause. Oral notification to the Contracting Officer shall be confirmed in writing within ten days of the oral notification. To contact the Contracts Office, call (505) 665-9175.



Russell K. Kirkpatrick
Assistant Manager
Security Management



Robert M. Poole
Contracting Officer

cc:
SM File
CO File, LASO
Records Center, LASO



Department of Energy
National Nuclear Security Administration
Washington, DC 20585



JAN 27 2000

MEMORANDUM FOR DISTRIBUTION

FROM: LINDA R. WILBANKS, Ph.D. *Linda Wilbanks*
CHIEF INFORMATION OFFICER

SUBJECT: Computer Loss/Theft Reporting Requirements

Effective immediately, the loss or theft of any piece of computer equipment that has the capability to store information must be reported to the DOECIRC within 24 hours, even though this is not categorized as reportable within the NAP 14.1-C.

The incident is to be reported even if the type or quantity of information stored on the equipment is unknown; updates should be provided as new information becomes available.

The requirement will be included in the next update to NAP 14.1-C, but until that time, this memo is direction for this additional reporting.

If you have any questions, please contact Wayne Jones at 202-586-9728 or e-mail at Wayne.Jones@nnsa.doc.gov.

Distribution:

James Cavanagh – NA-1
Bradley Peterson – NA-1
Gerald Talbot – NA-17
All Site Office Managers
All Site DAAs
All Site CIOs
Wayne Jones – NA-2.2





DEPARTMENT OF ENERGY
National Nuclear Security Administration
Los Alamos Site Office
Los Alamos, New Mexico 87544



FEB 03 2009

Mr. Michael Anastasio
Director
Los Alamos National Security, LLC
PO Box 1663, MS-A100
Los Alamos, NM 87544-1234

Mr. Rueben M. Rafferty
Prime Contract Office
Los Alamos National Security, LLC
PO Box 1663, MS-722
Los Alamos, NM 87544-1234

Dear Messrs:

Reference: Contract Number DE-AC52-06NA25396, Los Alamos National Security, LLC
(LANS) and the Department of Energy, National Nuclear Security Administration

Subject: Cyber Security / Property Management Concerns

Los Alamos National Laboratory (LANL) worked diligently over the past year to complete the demanding requirements of the Secretary's Compliance Order, and the National Nuclear Security Administration (NNSA) recently concurred that LANL had made great strides in improving the robustness of cyber security implementation. I feel this process also brought our organizations closer together as we worked toward common goals.

Cyber security requires continuous vigilance, which is evidenced by the unknown and unexpected that become matters of significance. For example, on January 16, 2009, three computers were stolen from a LANS employee's residence in Santa Fe. This incident has revealed several property management, accountability, incident reporting and cyber security concerns.

In treating this initially as only a property management issue, my staff and I, and apparently the cyber security elements of the laboratory, were not engaged in a timely and proactive manner to assess and address potential loss of sensitive information. Perhaps more frustrating is that, when this engagement did occur, significant uncertainty existed as to the state of compliance adhered to within the laboratory. This fueled greater concern as initial laboratory reports, which were reviewed at Headquarters (HQ) and at the Los Alamos Site Office (LASO), used vague terminology and made assertions that suggested significant weaknesses in individual controls, organizational management approval, accountability systems, configuration management, etc.

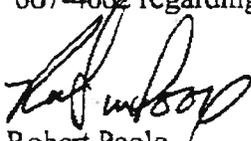
In subsequent follow-up to this and other emergent issues, LANS has reported that 13 computers have been stolen or lost in the past 12 months, and that 67 computers are currently "missing." The

magnitude of exposure and risk to the laboratory is at best unclear as little data on these losses has been collected or pursued given their treatment as property management issues as well.

In recognition of these events and their possible implications and in accordance with clause H-2 entitled performance direction, I am directing you to treat any loss of computer equipment with the capability to store data as a cyber security concern with reporting due to this office as outlined in the NNSA Chief Information Officer's (CIO) memorandum dated January 27, 2009. I am also directing the formal resolution of the status and potential cyber security ramifications of each of the 80 systems noted above be documented in a written report to me by Friday, February 6, 2009 close-of-business. Finally, I direct LANS to work closely with my staff to develop and execute an aggressive program to correct any system deficiencies/weaknesses in computer accountability and configuration management system consistent with the commitments resulting from the recently completed Security Compliance Order.

Please submit evidence packages to this office demonstrating the completion of this direction.

Please do not hesitate to contact me at (505) 667-5105 or Harold Brockelsby, DAA at (505) 667-4662 regarding this issue.



Robert Poole
Contracting Officer



Donald L. Winchell, Jr.
Manager

cc:

H. Brockelsby, CS, LASO
R. Kirkpatrick, SM, LASO
Records Center, LASO
Official Contract File, LASO

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 4.

What are the status and potential cyber-security ramifications of each of the 80 systems noted by the National Nuclear Security Administration in its February 3, 2009 letter to Los Alamos National Security, LLS (LANS)?

A 4.

The status of the 80 systems are as follows:

The original LANL report for calendar year 2008 identified 80 bar-coded pieces of computer related equipment being either stolen (13) or lost/missing (67). Since that report in early January 2009, LANL has since recovered or found through property/security/cyber security assessments 25 items, thus reducing the total to 55 lost/missing or stolen items.

As none of the 80 computers reported were used for classified processing, there was no potential compromise of classified information/systems. Investigations are still ongoing on 55 computers that have not been recovered. As such, the final cyber security ramifications have not been determined.

LANL/LASO POC:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 5 a.

What measures, protocols, or programs have been developed and executed to correct identified deficiencies?

A 5 a.

As directed by the Los Alamos Site Office, the Los Alamos National Laboratory has developed and executed the following measures to correct identified deficiencies:

- All lost or theft of computers and computer related equipment will be reported to a central Location, the Department's Cyber Incident Response Capability (DOE CIRC).
- In addition to the original report to the Security Incident Team, Physical Security and Property Management will contact the Security Incident Team if they receive a lost/stolen report for which no Security Call Assessment Record (SCAR) has been issued.
- Representatives from the Security Incident Team, Property Management, Physical Security, and Information Security, will be formed to review the Report of Lost, Damaged, Destroyed, or Stolen (RLDDS) process and form.
- Quarterly lost/stolen reports will be provided to LANL and LASO senior and line managers, for informational reviews.

Q 5 b.

How will these measures, protocols, or programs correct identified deficiencies?

A 5 b.

The measures identified above will ensure that the impact of missing equipment will be properly evaluated and reported in a timely manner, within the proposed technical and management chains.

LANL/LASO POC:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 6.

How many staff does the National Nuclear Security Administration have dedicated to cyber-security monitoring and oversight at Los Alamos National Laboratory, particularly those staff responsible for evaluating lost property risks?

A 6.

The Los Alamos Site Office is authorized three federal and three contractor positions focused on cyber security. One Los Alamos Site Office staff member is the focal point for incident response and resolution who regularly addresses stolen/lost/missing computer equipment events as they arise. In the event that computer equipment is reported lost, stolen, or missing, cyber security and physical security personnel will perform an evaluation of the risks associated with the information that resides on the lost property.

LANL/LASO POC:

Date:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

CONGRESSIONAL COMMITTEE ON ENERGY AND COMMERCE
QUESTIONS AND ANSWERS

Q 7 a.

Why would a Los Alamos National Laboratory employee have three government computers at his home?

A 7 a.

The three computers were used for three different purposes. The first computer, the Macintosh desktop, was used as the primary computer for work from home. The other two computers were laptops used for travel purposes. The first was a Macintosh used as a MacOS and Unix platform; the second a PC running Microsoft Windows. The two laptop computers provided the capability to interact with different research teams, and allowed compatibility checks of files generated by the two different operating systems. The content of the laptops was a subset of the contents of the desktop computer. Files were moved to one or the other laptop for specific travel purposes.

Further clarification regarding this question is as follows:

LANL tracks computing devices that are approved for off-site transport, which includes domestic and foreign travel and home use, through a Property Transport Request (PTR). As an example, an employee may be approved for multiple devices: one a laptop for travel for doing email correspondence and working on documents; desktop may be approved for offsite use for technical work in support of the activity he is authorized to do by his line manager.

All of the requests have been individually reviewed and approved to insure that they are appropriately justified for the work the individual is asked to perform.

Q 7 b.

How many LANL employees had more than one government computers at home prior to the incident?

A 7 b.

709 individuals had more than one computing device in their homes prior to the incident.

Q 7 c.

How many LANL employees currently have more than one government computer at home?

A 7 c.

LANL tracks computers that are approved for off-site transport. This includes domestic and foreign travel as well as home use. 552 employees have more than one computing device approved for off-site use.

Of the 552 approvals for off-site usage, 441 are approved for two computing devices most of which are a laptop and a PDA/Blackberry.

LANL/LASO POC:

HQ Program Office Approval POC:

Dr. Linda Wilbanks

Date:

Date:

Changes/Concurrences:

NNSA GC:

NNSA CI:

CNDS:

DOE GC:

IM:

DOE CI:

CF:

culture at LANL. We are concerned that LANL does not truly know what information was on this equipment or that NNSA security personnel have the ability to find out anymore. Given the history with LANL's security oversight and attention this Committee has focused in this area, we expected a more appropriate level of security protocols would have been in place and followed appropriately.

We understand your site office has issued directives to tighten security and has sought to review whether additional deficiencies exist. To assist our own understanding of the situation, we would appreciate your providing the following answers and information by four weeks from the date of this letter:

1. What were the lost property protocols followed by LANL management, Los Alamos National Security, LLS (LANS), during the time of the computer thefts cited in this letter, how long had they been in place, and what deficiencies did NNSA identify?
2. Had NNSA previously evaluated these protocols? If not, why not? And if so, what did NNSA determine?
3. What directives did the NNSA site office issue? Please provide any memoranda related to these directives, including, but not limited to, the NNSA Chief Information Officer memorandum dated January 27, 2009.
4. What are the status and potential cyber-security ramifications of each of the 80 systems noted by the NNSA in its February 3, 2009, letter to LANS? Please provide any written reports to NNSA relating to this request.
5. What measures, protocols, or programs have been developed and executed to correct identified deficiencies and how will these correct them?
6. How many staff does NNSA have dedicated to cyber-security monitoring and oversight at LANL, particularly those staff responsible for evaluating lost property risks?
7. Why would a LANL employee have three government computers at his home? How many LANL employees had more than one government computer at home prior to the incident? How many LANL employees currently have more than one government computer at home?

We would respectfully request, if the Department withholds any documents or information in response to this letter, that a Vaughan Index or log of the withheld items be attached to the response. The index should list the applicable question number, a description of the withheld item (including date of the item), the nature of the privilege or legal basis for the withholding, and a legal citation for the withholding claim.

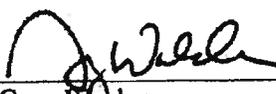
Letter to Mr. Thomas P. D'Agostino
March 27, 2009
Page 3

Should you have any questions, please contact Mr. Peter Spencer of the Minority
Committee staff at (202) 225-3641.

Sincerely,



Joe Barton
Ranking Member



Greg Walden
Ranking Member
Subcommittee on Oversight and Investigations

cc: The Honorable Henry A. Waxman
Chairman

The Honorable Bart Stupak
Chairman
Subcommittee on Oversight and Investigations