Testimony of John C. Browne
to the Senate Committee on Armed Services

June 21, 2000

Subject: Security Issues at Los Alamos National Laboratory

Introduction

Mr. Chairman and Members of the Committee:

I am John Browne, Director of Los Alamos National Laboratory. I am here today to report on a serious loss of control over classified information at my Laboratory.

As you know, the material in question was found on June 16 at the Laboratory in an area that had been previously searched more than once. As of this time, I have no knowledge that the information has been compromised or tampered with, or that espionage is involved. From a national security perspective, these are positive indications. They do not, however, relieve my anger and frustration over this incident. Nor do they diminish, in any sense, accountability for the loss of control in the first place or responsibility to

address the root causes that led to this incident. Accountability and responsibility belong to the Laboratory and me.

Unfortunately, this incident overshadows the hard work of 10,000 Laboratory workers who have contributed to significant security improvements over the past year – improvements that led DOE's Office of Independent Oversight and Performance Assurance to give us a rating of "Satisfactory" – the highest of three possible levels – at the end of 1999. There have been scores of other audits and reviews that have recognized the improvements we have made. It is difficult for me to fully convey my sense of frustration at the damage a single act – apparently human error or intentional wrongdoing – can do to the accomplishments of so many.

There are three key messages I want to emphasize today:

- We are accountable. Corrective actions are underway; disciplinary actions will be taken, subject to the immediate requirements of the ongoing criminal investigation.
- We offer no excuses. We will identify and aggressively address root causes.
- Outstanding science is necessary – but it is not sufficient. Arrogance, indifference, or carelessness, regardless of an individual's or an organization's accomplishments, will not be allowed to compromise our nation's security.

Background, Incident, Immediate Reaction

I will give you as clear a version of the situation as I can consistent with security requirements and the state of the criminal investigation. My comments and conclusions are very provisional. As the investigation proceeds and our understanding develops, I expect that our thinking will change.

Let me begin with some brief background:

First, the hard drives that were missing are, of necessity, easily portable. The information they contain supports operations of the Nuclear Emergency Search Team – a DOE program that involves the three Defense Programs laboratories and other organizations. Its members are on call 24-hours/day, 7 days/week. When they are mobilized, the hard drives in question are removed from the Laboratory as required. In fact, they have been removed many times in the past, and always control has been maintained.

Second, the de-emphasis on formal accountability of classified documents across government that began in the early 1990s, in my opinion, weakened some security practices and led to an atmosphere that countenanced less rigor and formality in the handling of classified information. I am not suggesting that this is an excuse for what happened. I believe it is, however, a contributing factor.

Third, I believe there has been confusion in the chain of command as it involves NEST. Again, I do not suggest this ambiguity is an excuse nor do I believe it is a root cause for our loss of control. Ambiguity, however, heightens the risk that security procedures will not be as effective as might otherwise be the case.

Fourth, I reject the notion that this event demonstrates an irreconcilable conflict between scientific excellence and effective security. I also strongly disagree that this incident lends credence to the suggestion that the University of California should not continue to manage DOE's defense laboratories

As to the timeline of this incident, the following information is what I currently understand: The last formal audit of the hard drives occurred in early January as part of a

Y2K audit. There was an undocumented confirmation that the hard drives were in the NEST toolkit on April 7, and a possible confirmation of their presence on April 27. Neither of these facts gives me much confidence.

On the evening of May 7, as the Cerro Grande fire threatened the Los Alamos townsite and the Laboratory, two NEST team members requested permission to enter the X-Division vault from my Deputy Laboratory Director for Operations who was the Emergency Director in charge of our Emergency Operations Center. He granted this access based on the NEST team argument that the NEST toolkit must be relocated to a safer environment in case of the need to respond to a national emergency. The NEST team members apparently found the two hard drives missing, replaced them with two backup drives, secured the vault, and moved the NEST toolkit to another location. They made a major mistake in that they did NOT notify Laboratory senior management of the missing hard drives at that point.

From May 8 to May 22 the Laboratory was closed for fire emergency operations and only fire fighters, security, and necessary operational people were permitted into the Laboratory. We began to reopen the Laboratory on May 22 with most people re-occupying their facilities by May 24. On May 22, at least one member of the NEST entered the vault but did not notify senior management again about the missing hard drives – a second serious mistake.

On May 31, after failing to find the missing hard drives, the line management of X-Division was notified. The X Division Director notified the Deputy Associate Laboratory Director for Nuclear Weapons who, in turn, notified Laboratory security (S Division). Our

S-Division personnel began a confirmation process to determine if the hard drives were actually missing or not.

Around noon on June 1, my Associate Laboratory Director for Nuclear Weapons (ALDNW), the senior manager on my team responsible for all nuclear weapons work at the lab, was notified that the hard drives were missing. He took immediate actions to visit the vault and to plan a response. In the afternoon of June 1, ALDNW and the Deputy Director of my Security Division notified me of the missing hard drives. I directed the Security Division Deputy to immediately contact the Department of Energy in compliance with the Department's 8-hour notification rule. The fax was sent at 5:07 pm on June 1 and received by DOE/HQ/Emergency Operations Center at 5:08 pm. It is clear that there was a lengthy delay, internal to the Laboratory, in notifying me, the Associate Laboratory Director, the Security Division, and possibly others by those who had been aware of the missing hard drives since early in May. That delay is plainly and absolutely unacceptable. The timeline is of serious concern and must be understood to determine the root cause of the delay.

On June 2, I held a videoconference with DOE Deputy Secretary Glauthier and other DOE officials to plan a course of action. We launched a massive search on Friday and throughout the weekend of the X Division, other LANL locations, other DOE sites, and any possible external NEST storage site. Safes, vaults, and offices were checked numerous times by many different individuals. Our Security Division conducted over 200 interviews of 85 people who had escorted or unescorted access to the NEST vault in question. On June 5, I formally requested assistance from the DOE and FBI during an early morning videoconference with the DOE Deputy Secretary. He immediately tasked Gen.

Habiger to assemble a joint team with the FBI. Gen. Habiger arrived the next day and took over the inquiry.

Immediate Actions

Immediately after I found out about the missing hard drives on Thursday June 1, I initiated all actions that were required, prudent to limit further damage, or appropriate to facilitate further inquiry. These actions included:

- Notification of the DOE.
- Directing an independent search with multiple two person teams, from June 1-4.
- Directing interviews of all available individuals with vault access -- 85 people were interviewed a total of 200 times by our security personnel.
- Standing down X Division to do two-person searches of safes, vaults, and offices.
- Closing and sealing the NEST vault.
- Requesting FBI involvement through the DOE.

Follow-up Actions

I initiated the following actions in the week following the June 5th period.

- Reviewed operations of all 96 LANL vaults.
- Expanded logging of all vault entries and exits
- Changed all vault lock combination
- Reduced access lists for vaults and Limited Access Control Areas (LACAs).

- Began placing barcodes on all high-density computer storage media with SRD to facilitate inventory.
- Reviewed all nuclear weapons programs to ensure that they have security plans consistent with DOE and Laboratory policy.

These activities addressed immediate concerns, but we recognize that more may need be done. We are working with the DOE to identify and implement additional measures that address root causes.

In addition, I asked the University of California to undertake an immediate, independent review of the security management related to this incident. Pending completion of that review, I directed that six managers – the entire management chain related to the program, vault operations, and hard drives – be placed on leave with pay. My action in this regard was intended to assure the unquestioned independence of the University of California review process. The leave was not disciplinary or investigative, and did not prejudice the position or performance of any of the individuals.

Unfortunately, just as the University of California review was getting underway, we were directed by the Department and the FBI to suspend it. I fully understand the reasons for the DOE's direction – namely, to avoid all possible interference or conflict with the ongoing criminal investigation. Obviously, the criminal investigation must take priority. We do not know when or if the UC review will resume. In the meantime, I have asked the two most senior of the six managers to return to work and resume their duties for managing the nuclear weapons program. I am continuing to review the status of the four remaining on leave.

Security Emphasis

This matter is extremely painful and disturbing to me because of the potential damage to national security. I am outraged that this happened at Los Alamos after the events of last year. There is no excuse. This event overshadows the improvements we have made in security in the last two years through the investment of additional resources and the hard work of almost every one of the 10,000 workers on site. The improved status of our whole security posture, physical and cyber, was validated by the DOE's Office of Independent Oversight and Performance Assurance at the end of 1999 with a rating of "Satisfactory," the highest of their three rating levels, following a year of preliminary visits and final audits. The GAO followup report, "Improvements Needed in DOE's Safeguards and Security Oversight" (February 2000) primarily addressed integration of oversight findings and followup records. The GAO report calls out a noteworthy practice that Los Alamos maintains its own database with "virtually every known security problem at the laboratory."

Some of the measures taken by the DOE and the Laboratory in the past two years include:

- Implementation of the DOE polygraph program under Edward Curran, DOE Director of Counter Intelligence.
- Intensified security awareness training -- including automatic rejection of personnel at entry badge readers if their training is overdue.
- Took strong disciplinary actions for all security infractions as appropriate including termination, leave without pay, suspension of access, and reprimands.

- Strict site and cyber access for foreign nationals.
- Network separation with firewalls between Laboratory administrative computing and public information computers -- an additional layering beyond complete isolation of the classified computing network completed six years ago.
- Eliminating authorized use of any computer for both classified and unclassified computing (dual-use computers eliminated).
- Enhancing classified parts storage.
- Raising the security and safeguards function to division status in the Laboratory; creating a separate counterintelligence office reporting to the Office of the Director.
- Filling both of these leadership posts with experienced professionals.
- Estabishing an information security policy board that has laid out a comprehensive cyber security program on which we have made significant progress.

Actions by the University of California Office of the President (UCOP) include appointing a security advisory panel chaired by Adm. Tom Brooks and appointing a security director, Terry Owens, for contractor oversight. The UCOP and Admiral Brooks has assembled an outstanding panel that has begun to evaluate security practices across a broad spectrum at the two UC weapons labs.

These actions and the intense scrutiny that this Laboratory underwent last year with scores of independent audits and reviews did not help us prevent this incident. The NEST program in question has features that inadvertently may have reduced the Laboratory's

institutional controls and helped set the stage for serious errors. Nonetheless we cannot excuse individual accountability if it is found that responsibilities for protecting this information were not properly carried out.

NEST

The Nuclear Emergency Search Team (NEST) is a DOE operation involving the three DP Laboratories and other organizations inside and outside of the Department with close coordination and oversight from headquarters. This arrangement, unless very carefully structured and overseen, has the potential to undercut line management authority. NEST mobile equipment includes portable computers so that the team can perform their duties at remote sites. Removable hard drives facilitate transport of the information for NEST deployments and for information updates. Team members are on call 24 hours per day with a tight timeline for response. These hard drives were removed from the LANL site many times in the past and accountability was maintained in prior movements.

The NEST program limits knowledge of activities to those individuals with detailed involvement. There are features similar to Special Access Programs (SAPs) but without the same level of security oversight by the sponsor and formality of operational security that SAPs have. When NEST deploys, control shifts from one headquarter unit to another to DOE. This arrangement can create confusion about who is charge at what point in time.

Uncertainty in authority and responsibility, especially for such a critical function as security, must not be allowed to occur. DOE has recently clarified this situation in a letter that documents that responsibility for proper security procedure rests with the national laboratories for all activities performed at the laboratory or under laboratory auspices.

There is a model for security management used for programs with similar needs that could be applied, as I will discuss later.

I want to reiterate that I do not believe that the NEST situation described above is an excuse for this incident, or that it even contributed directly to it. A full root cause analysis is needed.

Security Requirements

The NEST program generates and uses secret restricted data (SRD) within an authorized security area with authorized storage containers. Those are the only requirements that need to be met. Use of Limited Access Control Areas (LACAs) and vaults for the SRD used by NEST and other activities provides enhanced protection. These measures provide additional measures of protection against access by persons without an immediate need-to-know.

LACAs and vaults are additional layers of protection when used inside an SRD security area. Our requirements for their implementation and use included provision of substantial physical security outside of normal work hours.

The requirements for daytime access control for the NEST vault in question were largely administrative. Any person on the primary list-- 26 people -- was authorized to make unaccompanied entry. Any person on the secondary list -- 57 people -- was authorized to enter if escorted by a person on the primary list. There was no DOE or Laboratory requirement to log individual personnel entries or record removal of classified materials, unless it was to be removed from all three layers of protection—the vault, the LACA, and the SRD security area.

Unique identification and inventorying of secret documents was a government-wide requirement prior to 1991. As the increasing volume of secret documents consumed more resources just to inventory, the government progressively downgraded requirements. In 1992, the inventory requirement for SRD was eliminated. LANL implemented the SRD inventory change in 1993. Additionally, the DOE requirements for transport of SRD outside of secure areas do not provide for a unique identification of the item transported.

Possible Causes and Lessons Learned

Organizational considerations are very important in this incident. We do not believe that the NEST relationship between the DOE headquarters office and the Laboratory was sufficiently formalized so that authority, responsibility, and accountability were tied together. A suitable framework already exists with Special Access Programs (SAPs). We execute many programs with DOE and other sponsors under this arrangement, which follows a strict protocol. Consideration must be given to putting NEST and all other less formalized programs into such a relationship.

The de-emphasis on formal accountability of classified documents that occurred across the government early in the '90's, in my opinion, weakened our security practices and set up an atmosphere that leads to less rigor and formality in handling of classified information.

Over this time, the issue of security vulnerabilities opened by high-capacity digital storage and transmission has not been adequately reflected in established requirements, but as mentioned earlier, we are addressing this concern with immediate practical action. This whole issue needs government-wide consideration.

Longer Term Actions and Recommendations

Our immediate corrective actions were covered above. Some of these, such as barcoding high-density computer media for inventory, have continuing high importance. Longer-term actions under consideration include:

- Automatic electronic logging of access into LACAs and vaults
- A higher level of control of movement of classified items
- Strengthened protection of information in high density storage by change of classification or use of advanced technical means (such as encryption).

Our recommendations for more general improvements include:

- Government-wide review of the security vulnerabilities associated with high-density storage and high-speed transmission of digital information, with development of standards and requirements to follow.
- Ensuring that limited access programs have the necessary formality assigning responsibility and authority between the Laboratory and headquarters.

Concluding Remarks

As Director of the Laboratory, I recognize the seriousness of this security incident and in my position I recognize that I am accountable for the actions of my Laboratory. I am committed to taking the strongest possible actions I can to secure the nation's nuclear secrets.

These actions will include disciplinary actions up to and including termination of employment against individuals who willfully or carelessly violated the rules. If there were criminal charges filed against any individuals those would be handled in the courts. There

will be a message that security rules apply to everyone here. No level of expertise or insider knowledge can justify departures from our security requirements.

The actions I have taken and will take are based on the need to limit further damage and address root causes to prevent reoccurrence. Among the root causes I have identified are weak controls on document inventory, lack of formality for certain limited access programs, and human failure. We are committed to living up to our security responsibilities. We have made tremendous strides forward in the last two years. With your support this incident too will be overcome. If we act with wisdom, the Laboratory and our nation's security will in the end emerge stronger.