Statement of Thomas P. D'Agostino
Acting Administrator
and
Deputy Administrator for Defense Programs
National Nuclear Security Administration
U.S. Department of Energy
Before the
House Committee on Energy & Commerce
Subcommittee on Oversight & Investigations

January 30, 2007

My name is Thomas P. D'Agostino. I am the Acting Administrator of the National Nuclear Security Administration (NNSA), within the U.S. Department of Energy (DOE), a position that I have held since January 20, 2007, upon the resignation of Ambassador Linton F. Brooks. I realize that one of the primary reasons I am in this position is because of the Secretary of Energy's dissatisfaction with progress in management and security issues, notably related to Los Alamos National Laboratory (LANL).

Let me be clear, all options for both penalties and motivation are under consideration with LANL. This is not an academic exercise with a nominal fee at stake—the maximum available annual fee for operating LANL, with safety and security as key factors, is over $70 million. The majority of Los Alamos National Security LLC's (LANS) fee is at risk as is their ability to earn additional award terms. The combination of award fee and award term are powerful incentives on performance and I intend to fully utilize these in managing the contractor. The Department is conducting a review of the incident to determine whether a Notice of Violation will be issued. Finally, the contract

has a clause called "Conditional Payment of Fee, Profit, and Incentives." This clause allows for the complete elimination of fee in the event of a serious safety or security event that results in the loss of life or grave and irrecoverable harm to the security of the United States.

I am serious about my new responsibility for security across the nuclear weapons complex. In fact, my first two days on the job as Acting Administrator were spent in New Mexico at LANL and the Los Alamos Site Office (LASO) to get a first hand, upfront and personal appreciation of the issues and to talk with the people responsible for implementing improvements. I was at the Site Office to see the staff and personally explain my recent decision to reassign the Site Office Manager, Ed Wilmot. In Mr. Wilmot's place, I have directed one of the Department's most experienced Site Office Managers, Mr. Dan Glenn from the Pantex Site Office in Amarillo, Texas, to serve as the Acting LASO Manager until a permanent replacement is found. Mr. Glenn has extensive safety and security experience at one of our most sensitive facilities; in fact, Pantex is the only NNSA facility where we have complete nuclear weapons on-site. LANL is also a unique place with some of the world's best science and most sensitive information, and I will support LASO with the best team to continue to drive improvements and make sure we are getting the job done.

On January 3, 2007, I notified the LANS Board of Governors Executive Committee that I was calling the Executive Committee to Washington, D.C. that following week. On January 10, I met with the Executive Committee and told them of

my concern in how they have handled the current security incident at LANL. The Secretary, Deputy Secretary, NNSA Administrator, and LASO Manager joined me to emphasize the seriousness of the situation. In the coming months I will be routinely meeting with members of the Executive Committee to hear how they will to improve the security culture at LANL. Additionally, I have asked the Chairman of the Board of Governors, Mr. Gerald L. Parsky, to call the Secretary on a regular basis to update him personally on actions that the Board takes to reach back to the corporate parents to support improvements at the laboratory.

Make no doubt about this—if the current laboratory management is unable or unwilling to change the security culture at LANL, I will use every management tool available to me, consistent with the terms of the LANL contract, including recompeting the contract if necessary.

All NNSA security functions, with the exception of cyber security, are consolidated under the NNSA Associate Administrator for Defense Nuclear Security. All NNSA cyber security issues are consolidated under the NNSA Chief Information Officer, who reports to the NNSA Associate Administrator for Management and Administration.

With respect to the current issue of security at Los Alamos, let me assure you that NNSA is committed to the security of our nuclear weapons, nuclear material, and classified matter and it has taken significant steps to improve security since its inception. Neither NNSA nor I take any breach of security lightly.

The nature of our classified operations is complex, but the elements of good security are not. Good information security entails clear rules, strong controls, testing and validating, which provides for a credible deterrence. Personnel security clearances determine who gets access to classified information. Building and security area access controls provide high confidence that people going in and out of classified work areas are authorized to be there. Information security controls work to ensure that only people with a need to know have access to the information.

While these controls help set the foundation for a good security program, the system must also provide deterrence against violations of the rules and controls; a high probability for the discovery of security violations; and strong sanctions for willful or negligent violations. While we expect that security-cleared employees will abide by security rules because they understand and value good security, the system must also provide credible deterrence against intentional or inadvertent violations of the system of rules and controls. Searches and work area spot checks help to ensure the system is operating as designed across all levels of the operation. We must continue to strengthen these activities. Specifically, LANL has strengthened its security escort requirements and more clearly specified the expectations and requirements for their escort program. LANL has also increased the number of inspections of personnel entering, working in, and exiting security areas and have conducted nearly 5,000 additional inspections since this incident came to light.

While the Secretary has commissioned a special task force to review the Department's personnel security program, NNSA has been taking action over the past year and a half to improve our personnel security processes. Specifically, we re-engineered work practices to reduce clearance processing time, implemented the electronic questionnaire for investigations processing (e-QIP), strengthened our quality assurance mechanisms, and instituted metrics to monitor and report on the performance of our personnel security functions. Additionally, we have coordinated with the Defense Security Service to provide comprehensive clearance adjudication training to our nearly 100 contractors and Federal personnel security professionals at the NNSA Service Center.

During the past two years, NNSA has made changes to strengthen the cyber security posture across the national complex and more recently has addressed issues identified by the LANL incident. During 2005, the Department developed the strategic plan and a deployment schedule for Diskless Workstation implementation. In 2006, the Agency appointed Designated Approving Authorities (DAAs) for each NNSA site who are dedicated solely to cyber security, policy oversight and inspection.

NNSA has also assembled its Federal cyber security experts from across the Complex to inspect all Vault Type Rooms at LANL to determine their compliance with the Department's directive to close vulnerable system data ports. We have also set in place a schedule for this team to inspect the cyber security implementation at all other NNSA sites. Based on these inspections, I plan to take aggressive actions to strength our

cyber security and I pledge to you that I will deal as swiftly and directly with any incidents or actions that are needed to improve the cyber security posture of the NNSA.

I would like to highlight some of the actions NNSA has taken to improve security, most notably those taken since the last significant security incident at Los Alamos in 2004, involving Classified Removable Electronic Media (CREM).

NNSA completed two major studies of NNSA security, one led by Admiral (Retired) Hank Chiles and one led by Admiral (Retired) Rich Mies. Admiral Chiles' report in March 2004, "Strengthening NNSA Security Expertise: An Independent Analysis," provided recommendations to make our Federal security workforce more effective. Admiral Mies' study in April 2005, "NNSA Security: An Independent Review," provided more than 100 recommendations in 13 programmatic areas, including physical security, cyber security, intelligence and counterintelligence and making recommendations ranging from program management to budgeting to oversight.

In response to the Chiles report:

- Our Federal Site Offices have implemented formal security training programs leveraging the Department's Technical Qualification Program and the DOE National Training Center's Professional Enhancement program.
- We established a security intern program and have successfully integrated it into the Department's Future Leaders Program.

Likewise, we took effective action to implement the recommendations of Admiral Mies by:

- Partnering with DOE's Office of Health, Safety, and Security to review our security policies with the goal of making our policies consistent with national standards, clearly understandable, and effective when implemented;
- Re-aligning Defense Nuclear Security staff roles and responsibilities to improve security program planning, programming, and evaluation;
- Issuing a Performance Assurance Program, which provides a multi-tiered system of self-assessments and other reviews of security performance aimed at assuring comprehensive assessments of security programs;
- Establishing the Defense Nuclear Security Leadership Council, which comprises all site office security directors and meets regularly to address overarching security implementation challenges;
- Actively disseminating lessons learned from incidents and inquiries and the Associate Administrator for Defense Nuclear Security has directed the establishment of a Security Lessons Learned Center which will enhance our information sharing; and,
- Replacing several Federal security directors for sub-standard performance.

We have received a number of reports from the Government Accountability Office, the DOE Inspector General, and the DOE Office of Independent Oversight. Like the Chiles and Mies studies, we have addressed the recommendations in these reports and have made major improvements.

However, we do not rely on others to identify ways to improve security. You will recall that in 2005, the Administrator announced his intention to stand up an NNSA Headquarters Security Oversight Office. Over the course of 2005 and 2006, that office has been staffed and has begun conducting regular and special reviews to ensure the effectiveness of our security programs and security line management. This office is also implementing our new risk management model and the oversight of security planning and vulnerability analysis. It has improved our responsiveness to outside recommendations, reduced the number of open findings, and reduced the number of security incidents across the complex through a more effective sharing of best practices and lessons learned. This year we will begin our first review of Site Office oversight processes as part of an initiative to improve our local Federal security oversight even more.

Again, I take these most recent events at LANL very seriously. I welcome suggestions on how to best proceed at LANL and want to have a national laboratory that is known best for its outstanding contributions to national security and the advancement of science.