Testimony of Glenn S. Podonsky
Chief Health, Safety and Security Officer
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives

January 30, 2007

Mr. Chairman and members of the subcommittee, thank you for inviting me to testify today as you probe into the security violation involving the improper removal of classified information from the Los Alamos National Laboratory. To perform its national security mission, the Department of Energy produces, processes, and stores significant quantities of classified material on a continuous basis. Because of the nature of this information and its potential impact on the national security of the country, we need to ensure that our policies and practices minimize the risk of potential security failures.

In light of the progress made in the last few years throughout the Department to correct past performance deficiencies in the control of classified information, this most recent unauthorized removal of classified information by a cleared employee at Los Alamos is a significant disappointment to the Secretary and the Department. We fully understand that incidents such as the one currently under examination by the Committee not only expose our sensitive national security information to potential compromise, but erode public confidence. As an organization with a mandate for an independent review responsibility, our organization is responsible for assessing performance based on the facts.

Los Alamos has made some progress in the past five years, but we must balance this against what should be the expectation of performance for an organization with such a critical scientific, defense and national security mission. In this respect, Los Alamos has been slow to address the root causes of its failures and to transform the entrenched operational culture that perpetuates them. Los Alamos now has new contractor management and an opportunity to move in a more positive direction.

At the time this specific incident was discovered, the Office of Independent Oversight was conducting a scheduled comprehensive inspection of the Laboratory's safeguards and security, cyber security, and emergency management programs, including those responsible for protecting classified information. Consequently, the Office of Independent Oversight was not assigned responsibility for conducting the inquiry into the circumstances surrounding the incident. This responsibility was assigned to the Inspector General. I will therefore focus my remarks on the overall performance of the programs we observed during the Independent Oversight inspection of Los Alamos National Laboratory.

Prior to our recent inspection activity, we conducted inspections of safeguards and security, cyber security, and emergency management programs at Los Alamos in 2002. The 2002 safeguards and security inspection determined that the Laboratory's Material Control and Accountability program was performing at less that an effective level of performance. During the concurrent cyber security inspection, the classified cyber security program was determined to be performing effectively, consistent with DOE requirements; however, the unclassified cyber security program exhibited significant weaknesses.

Independent Oversight's 2006 comprehensive inspection of Los Alamos also covered the areas of safeguards and security, cyber security, and emergency management in compliance with current Independent Oversight protocols. On-site activities for the 2006 inspection concluded last month. The final inspection report is currently under review and has not yet been published. Although the final report has not been issued, we can provide a brief general summary of the major inspection results in terms that are appropriate for this unclassified hearing.

Safeguards and Security Programs

During this inspection, the Laboratory's safeguards and security programs exhibited both strengths and weaknesses. While we are encouraged by limited improvements in some areas, we believe that considerable work remains to be done to ensure that safeguards and security programs at Los Alamos fully meet Department expectations.

Protection of Special Nuclear Material

Our inspection concluded that Los Alamos is adequately protecting the Category I quantities of special nuclear materials. This is based on our observations of effective performance in several critical areas, including improved performance in some functions that had previously exhibited weakness in 2002. The most significant improvement in the protection of special nuclear materials can be attributed to the collective actions of the Department, NNSA and Los Alamos to remove weapons grade quantities of this sensitive material from Technical Area 18, which had been the target of much public criticism for several years regarding its questionable security posture. The transfer of a significant quantity of material to the Nevada Test Site's Device

Assembly Facility, a substantially more secure facility, has facilitated on-site consolidation of weapons grade materials into a single security area at Los Alamos that affords a more effective protection posture.

Physical security systems installed to protect special nuclear materials at Los Alamos were subjected to rigorous performance testing and evaluation. Though aging, the current Perimeter Intrusion Detection and Assessment System around the facilities processing weapons grade special nuclear material performs effectively, and is adequately maintained.

Our evaluation of the Laboratory's protective force identified improvements since the 2002 inspection. Many of these are attributed to the aggressive steps taken to meet Departmental security goals by the end of FY2006. For example, Los Alamos increased protective force mobility, survivability, and lethality (e.g., procurement and deployment of enhanced weapons systems and armored vehicles). Protective force members performed effectively in both Limited Scope and full scale Force-on-Force performance tests. While overall protective force performance was determined to be effective, additional attention is required to improve certain tactical capabilities and communications.

While the Material Control and Accountability Program showed the greatest level of improvement since the 2002 inspection and was deemed to be performing effectively, some program areas require further attention, including the vulnerability assessment process which identifies risks associated with small quantities of nuclear materials maintained outside of the Protected Area. In addition, processes to accurately measure certain nuclear materials that

present unique measurement uncertainties require further work. Continued programmatic support is needed in order to sustain program improvements.

While not currently placing nuclear materials at risk, a few elements of the protection program for special nuclear materials require increased management attention. For example, several aspects of the Human Reliability Program require strengthening. This assurance program monitors the trustworthiness and reliability of employees who perform sensitive duties and require physical access to weapons-usable special nuclear material. Similarly, various aspects of the issuance and retrieval of security badges and the out-processing of employees need to be improved. These elements require increased attention and follow-up by line managers.

Protection of Classified Matter

In the area of classified matter protection it was evident that the site has made significant improvements in its efforts to track and account for Classified Removable Electronic Media and printed documents, is implementing a new electronic lock and key system that will reduce the number of keys and will record key usage, and has implemented a security inquiries program that provides stable leadership, is thorough in its process, and uses results in the form of lessons-learned to avoid recurrence where possible. While certain elements in place to protect classified documents and materials were found to be functioning effectively, we identified a number of significant problems within this program.

It was evident that the site is overly dependent on the use of non-standard storage configurations for the protection of many of its classified weapons parts. Storage of classified weapons parts at Los Alamos does not meet normal protection requirements and therefore required alternative protection measures to adequately compensate for storage configuration shortcomings. Compensatory measures that were specifically established to support approval of these non-compliant storage configurations were found to be inconsistently executed and were therefore not providing adequate protection. Furthermore, the need for additional protection measures was also identified in order to ensure that some classified components were protected from unauthorized visual or physical access. A review of the Technical Surveillance Countermeasures Program, intended to protect against electronic eavesdropping, revealed that the program lacked the resources necessary to provide the levels of support required by the Laboratory and its missions. The overall impact of these and other deficiencies in the protection of classified matter at Los Alamos is considered to be substantial.

Management Feedback and Improvement Mechanisms

With regard to management processes, implementation of important management feedback and improvement mechanisms was seriously flawed at both the Laboratory and the NNSA site office. While the Laboratory has new plans for conducting self-assessments and implementing a contractor Performance Assurance Program as part of the contract transition, the plan has yet to be fully implemented. Neither has the Laboratory implemented an effective process for developing, implementing, tracking, closing, and validating corrective actions for identified deficiencies. Similarly, the NNSA site office's Security Survey Program – a primary tool for

line management oversight of contractor security performance – also suffers from insufficient resources and inadequate implementation. In a few cases, the Laboratory has decided not to comply with DOE requirements and the Laboratory and NNSA did not utilize the Department's mandated deviation processes to fully assess and accept the risks associated with these decisions. Additional effort is needed to improve performance of management systems, since these areas are essential to attaining and sustaining effective protection programs, not only in the safeguards and security arena but also in cyber security and emergency management programs.

Cyber Security Programs

Independent Oversight also inspected classified and unclassified cyber security programs at the Laboratory. We conducted penetration tests of unclassified systems during the 2002 inspection. However, this most recent inspection was the first time that classified computer systems at Los Alamos were tested in such a rigorous manner. (Independent Oversight was granted specific authority to conduct penetration testing of classified systems by the Deputy Secretary of Energy in 2004).

Some progress in improving Los Alamos cyber security was identified by our inspection team, the most significant of which include the segmentation of computer networks to establish need-to-know protection controls, implementation of measures to mitigate risks posed by wireless technology (on the unclassified network), and the centralization of management responsibility for most information systems. In addition, the unclassified computer network was identified as

deploying a well-configured perimeter defense that successfully mitigates many of the sophisticated threats originating from the Internet.

While progress was evident in certain areas, much improvement is still required to safeguard classified information. Los Alamos' cyber security policies and procedures are not comprehensive and are not up to date with DOE/NNSA requirements or other guidelines, nor do they sufficiently address threats posed by emerging technologies. Additionally, risk management processes are insufficient, resulting in risk acceptance decisions at inappropriate levels of management.

The protection of classified computer systems is overly dependent upon administrative controls rather than on more robust engineered controls and barriers. The existence of such measures would have mitigated the ability of the employee involved in the security incident to perform the actions necessary to remove the data from the classified computer system without authorization. Because the Laboratory has not implemented these measures, Los Alamos national security systems continue to operate at an increased risk from insider threats. My Office has been working with the Chief Information Officer in revising the Department's classified cyber security policy to address emerging technologies and new threats. The Chief Information Officer has made this effort one of his highest priorities.

Another problem area identified at Los Alamos involves the certification and accreditation of both classified and unclassified information systems. Los Alamos certification and accreditation processes have not kept up with current methodologies, and existing processes do not ensure a

consistent approach for applying and testing necessary security controls. There are 25,000 unclassified workstations and servers at Los Alamos not certified and accredited.

Moreover, self-assessment processes are weak, with very few systems actually being tested as part of these assessments. Deficiencies identified during self-assessments are not reported to the Los Alamos Site Office or NNSA, and development of corrective action plans to address them is optional. As a result, there is little in-depth understanding of program weaknesses. It is also of concern that the Los Alamos Site Office and NNSA have not provided sufficient leadership to ensure that all current cyber security requirements are appropriately implemented and that performance is monitored to ensure effectiveness.

While progress has been made to date, the cyber security issues that remain at Los Alamos make it clear that a significant amount of additional work is needed in this area.

Emergency Management Programs

Independent Oversight also conducted an inspection of Los Alamos' emergency management programs. Of the seven focus areas inspected, all were found to exhibit serious weaknesses requiring increased management attention. Inspection results reflected a lack of progress in implementing program improvements for previously identified deficiencies. More disconcerting is the fact that four previous findings, although closed by NNSA, had not been effectively corrected.

Other Related Independent Oversight Activities

Secretary Bodman has requested my office to organize and lead a joint task force to review the Department's overall Personnel Security Program and Policies. As we noted earlier, the recent Los Alamos incident raised DOE management concerns about certain determinations used in granting clearances several years ago. In addition to questioning processes used to adjudicate derogatory information, these concerns also involve the adequacy of follow-up procedures for monitoring and reinvestigation when warranted. This task force will review DOE's personnel security policies and standards and will provide specific findings and recommendations for resolving identified deficiencies. Task force activities are scheduled to be completed by February 28 of this year. In addition to performing these activities in the personnel security arena, my office will also support the Chief Information Officer, who has been assigned by the Secretary to conduct a similar review of the Department's Cyber Security Program. I will defer to my colleague, Mr. Pyke, to elaborate on his plans for the conduct of this cyber security review.

Concluding Remarks

Mr. Chairman and Members of the subcommittee, our recent Independent Oversight inspection resulted in the worst set of performance ratings for safeguards and security, cyber security, and emergency management collectively that we have seen at the Los Alamos National Laboratory in many years. That combined with the history of security problems at Los Alamos is of great concern to everyone. However, it would be an oversimplification to say that everything is wrong at the Laboratory and that they are incapable of protecting national security assets. The recent

inspection indicated that, on balance, special nuclear material and classified removable electronic media, two areas with historical weaknesses, have improved and were adequately protected. Improvements in these and other areas should be considered along with the remaining significant deficiencies identified during the recent Independent Oversight inspection.

Since the time when responsibility for managing site operations was transferred to the new integrating contractor, there is evidence to indicate that the new contractual relationship provides a better foundation for security emphasis. In comparison to past contract management processes, the new contractual arrangements and performance-based award fee structure provide increased incentives for the Laboratory contractor to implement an improved, compliant, and effective security program in the future. However, the overall security picture is still below departmental standards—an obvious conclusion from not only site events but also from the results of our most recent inspection activity. As our organization moves ahead in the continued evaluation of the Laboratory's performance, we are mindful of the issues at Los Alamos and their causes. We are cognizant that productive changes require our continued commitment to identifying the origins of breakdowns in the areas of security, as well as health and safety. We look forward to participating in the continued identification and resolution of Departmental problems, and seek to assist Line Management in pursuing clear paths for successfully implementing corrective actions. We hope to do this through our independent oversight activities.

SUMMARY

Testimony of Glenn S. Podonsky
Chief Health, Safety and Security Officer
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
January 30, 2007

- When this incident was discovered, Mr. Podonsky's Office of Independent Oversight was conducting an inspection of security and emergency management programs at the Los Alamos National Laboratory. Therefore, he will focus his remarks on the results of that inspection.

- The inspection resulted in the lowest set of performance ratings for security and emergency management topics at Los Alamos since 1999. However, the inspection concluded that special nuclear material and classified removable electronic media are adequately protected.

- Significant problems were identified regarding the protection of classified documents and materials and with the configuration of vault-type rooms. Compensatory measures established to support approval of the non-standard storage configurations were inconsistent. The impact of the deficiencies related to the protection of classified matter was considered to be substantial.

- Cyber security policies and procedures are not comprehensive and are not up to date with DOE and NNSA requirements, and they do not sufficiently address threats posed by emerging technologies. Risk management processes are insufficient, resulting in risk acceptance decisions being made at lower staff levels that are inappropriate. In many cases, the protection of classified systems is overly dependent on administrative controls to mitigate potential adverse insider activity rather than by more robust engineered controls and barriers. The national security systems continue to operate at increased risk from malicious insiders.

- Los Alamos certification and accreditation processes for both classified and unclassified systems have not kept up with current methodologies, and existing processes do not ensure a consistent approach for applying and testing necessary security controls (25,000 existing unclassified workstations and servers were not certified and accredited). Self-assessment processes are weak, with very few systems actually being tested. Self-assessment deficiencies are not reported to the Los Alamos Site Office or NNSA and development of corrective action plans to address them is optional. A significant amount of work is required.

- Inspection results illustrate that there have been improvements, and that protection of the most important national security assets at Los Alamos, including special nuclear material and classified removable electronic media, are adequately protected. Nevertheless, significant protection and emergency management program deficiencies continue to exist at Los Alamos that require prompt, forceful, and sustained management attention and corrective action. NNSA and the Los Alamos Site Office, in particular, must considerably enhance their capabilities to effectively oversee contractor performance now and in the future.