

**Statement of Dr. Thomas O. Hunter
President, Sandia Corporation and
Director, Sandia National Laboratories**

**United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
September 25, 2008**

SUMMARY OF MAJOR POINTS

- Sandia has a longstanding culture of respect for security, rooted in a heritage of disciplined national service.
- The NNSA laboratories face a full spectrum of threats from multiple sources.
- The potential consequence of a terrorist organization obtaining a nuclear weapon or material is unacceptably high. We regard this prospect as the ultimate physical security threat. We regard the prospect of cyber attacks that have the potential to undermine the credibility of our nation's nuclear deterrent or that would allow a nation or other entity to develop a nuclear weapons capability as the ultimate cyber security threat.
- Sandia no longer possesses discrete Category I and II Special Nuclear Materials. These were eliminated by February 2008.
- Sandia was the first NNSA site to eliminate all discrete Category I and II Special Nuclear Materials, completing the project in February 2008, seven months ahead of schedule.
- Sandia controls and monitors all interactions between members of the Sandia workforce and foreign nationals.
- Sandia National Laboratories has three cyber environments, which are centrally managed and controlled.
- Sandia has taken many steps to improve cyber security in response to increased threats, providing an appropriate balance between protection and productivity..
- The balance of resources between physical security and cyber security has not yet been adequately adjusted to reflect the increased needs of cyber security.
- Sandia's experience in cyber security is a resource for DOE, its laboratories, and across many sites.
- In order to secure our cyber infrastructure, our nation must have a strong core of committed people with excellent skills supported with the necessary resources.

This page intentionally left blank.

**Statement of Dr. Thomas O. Hunter
President, Sandia Corporation and
Director, Sandia National Laboratories**

**United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
September 25, 2008**

INTRODUCTION

Mr. Chairman and distinguished members of the Committee, thank you for the opportunity to testify. I am Tom Hunter, president of Sandia Corporation and director of Sandia National Laboratories. Sandia is a multiprogram national security laboratory owned by the United States Government and operated by Sandia Corporation¹ for the National Nuclear Security Administration (NNSA).

My statement describes security program management and performance at Sandia National Laboratories. I will also comment on how we are responding to security issues of concern both to us and to oversight entities. I will give special emphasis to the challenges of cyber security.

Security Management at Sandia National Laboratories

Sandia has a longstanding culture of respect for security, rooted in a heritage of disciplined national service. The leadership at Sandia National Laboratories regards security as a central responsibility in the execution of our missions.

Our security program begins at the top of our Integrated Laboratory Management System. Safeguards and Security is a primary policy area managed by laboratory leadership, with oversight by the Sandia Corporation Board of Directors. Top management has established an

¹ Sandia Corporation is a subsidiary of the Lockheed Martin Corporation under Department of Energy prime contract no. DE-AC04-94AL85000.

unambiguous policy framework for security that is deployed through our management system to every organizational unit of the laboratory.

The security program at Sandia is structured with clearly stated lines of authority, responsibility, and accountability. Sandia's chief security officer integrates security policies and practices across the functional areas of physical security, cyber and information security, export control, and counterintelligence. These functional areas are managed by seasoned professionals in those fields, supported by expert staff. Because security can only succeed if it engages the workforce as a whole, we strive to maintain security awareness among our people through an active program of training and education. As a result, we have an expectation that our people will understand and comply with security policies and requirements, and we have a culture in which security is regarded as imperative. At Sandia, self-reporting of security incidents carries no shame (the majority of incidents are self-reported), and security processes are accepted as integral to programmatic work.

Security at Sandia is structured on the concept of defense-in-depth, a strategy of layered defense that we employ for both physical and cyber security. It begins with classifying assets and information into categories and levels based on sensitivity and risk. The government-wide classification system provides the foundation for our approach to protecting assets. We then apply protection systems appropriate for each category and level. Secret information will have more layers of protection than unclassified controlled information, and top secret information will have additional layers of protection beyond secret. We apply the need-to-know principle to information sets in both secret and unclassified environments.

In the past few years, Sandia has achieved significant success in strengthening the security program and instituting management reforms aimed at enhancing asset protection levels. I am pleased to report that our progress has been noted in recent inspections by the Department of Energy (DOE). The "Independent Oversight Inspection of Safeguards and Security" of August 2007 identified all major areas as "effective performance." The fiscal year 2007 Performance Evaluation Report by NNSA stated, "Sandia significantly exceeded performance expectations in the area of safeguards and security." While these comments are gratifying, we always pursue continuous improvement, and we actively work to improve our security posture.

The key to a secure enterprise is constant vigilance and a continuous and deep understanding

of threats and vulnerabilities. We cannot withdraw from the modern way of conducting business and performing research, and yet we must balance our need for modern information systems and flexibility with the imperative for security. The nature of our work differs from that in industry and academia, and our security challenge is somewhat unique.

We Face a Full-Spectrum Threat

The NNSA laboratories face a full spectrum of threats from multiple sources. Theft, espionage, sabotage, the insider threat, and carelessness are longstanding areas of concern. The physical avenues of these threats continue to require strengthening and attention. But the expansion of computer and communications technology over the last decade or so has opened whole new avenues of attack that are formidable and challenging.

Sandia has been programmatically engaged for decades in the study of threats that affect our national missions. In the early 1970s, the predecessor to DOE tasked Sandia National Laboratories to address the issues surrounding the potential for theft and sabotage of nuclear materials at DOE facilities or in transit. About the same time, the U.S. Air Force initiated a program at Sandia for research and development leading to the deployment of physical security systems for protecting globally deployed critical assets. It was during this period that Sandia began to acquire technical capabilities in security modeling and analysis, security hardware, and security systems engineering.

Although the cyber challenge is comparatively recent, we have addressed antecedents to modern cyber security through our decades-long engagement in use-control systems for nuclear weapons. Today we gain extensive insights into the evolving cyber threat via our programmatic ties to other agencies with responsibilities in this arena, and through our own analysis of the attacks directed to us.

Multiple threats exist today, and therefore they must be assessed and prioritized. For the purposes of this Committee, let me simply articulate the highest level threat I see for physical security and for cyber security:

The potential consequence of a terrorist organization obtaining a nuclear weapon or nuclear materials is unacceptably high. We regard this prospect as the ultimate physical security threat we face, and we defend most vigorously against it in our physical security systems.

Multiple threats similarly exist in the cyber realm—attackers range from amateur hackers to nation-states. Potential consequences can range from agency embarrassment to disablement of critical national security control systems. Cyber attackers sponsored by nation-states are not limited by budget, resources, and regulations, and they enjoy an asymmetrical advantage over time. We regard the prospect of cyber attacks that have the potential to undermine the credibility of our nation’s nuclear deterrent or that would allow a nation or other entity to develop a nuclear weapons capability as the ultimate cyber security threat. We defend against this prospect most vigorously.

We know that in both the physical and cyber arenas, an active insider would be an effective pathway for an adversary to accomplish its objective. Therefore, we place special emphasis on the integrity of our people and the role of counterintelligence as an integrated partner with our security programs.

Security Programs in Place at Sandia National Laboratories

Sandia manages its security operations in a systematic and disciplined way. We strive to comply with all applicable directives and requirements. We see compliance as the essential baseline—the platform from which we can advance our security performance.

Sandia’s assurance system for security management and performance applies the elements of Sandia’s Integrated Laboratory Management System at all Sandia sites. The Safeguards and Security Assurance Program provides management and oversight entities with an understanding of compliance and performance through analysis and trending of relevant data. We are working to enhance our trending capabilities by developing new metrics that provide more meaningful information. The key elements of the assurance system are self-assessments, performance assurance testing, and corrective action management. The assurance program helps management monitor the health of the security program, identify areas for improvement and design corrective actions, and ensure long-term sustainability.

Sandia’s security program implements short, mid, and long-term strategies aligned with the laboratory’s strategic plan and program guidance provided by the NNSA. The strategies are translated into prioritized goals with specific deliverables in our annual Safeguards and Security Implementation Plan, approved by DOE’s Sandia Site Office and monitored quarterly by

NNSA's Defense Nuclear Security Office.

Physical Security

An important objective in our physical security program has been to reduce the inventory of special nuclear materials (SNM) at Sandia sites. NNSA Administrator D'Agostino set a goal to consolidate SNM at five NNSA sites by 2012. Sandia was the first NNSA site to eliminate all discrete Category I and II SNM, completing the project in February 2008, seven months ahead of schedule. Sandia no longer possesses SNM in quantities that require a threat level 1 protection. This inventory reduction has made it possible for us to implement cost savings in our security program.

In 2007 Sandia placed a cap on the total number of vault-type rooms (VTRs) that would be allowed to exist to support mission activities. We initiated a project to examine the mission and security needs for every existing VTR. This rejustification project required line managers to look for opportunities to reduce classified holdings and consolidate and reduce storage locations, consistent with mission needs. To date, the VTR re-justification project has resulted in a 16-percent reduction in the number of VTRs at our New Mexico site and an even greater reduction at our California site.

Sandia's chief security officer has established a Sandia Security Footprint Advisory Council composed of senior managers from organizations across the laboratory as well as representatives from our Facilities group. The council is advising management on ways to effectively manage Sandia's security footprint and associated risks while assuring robust security.

Sandia controls and monitors all interactions between members of the Sandia workforce and foreign nationals in a fashion that is commensurate to the risks involved. All substantive relationships between Sandians and foreign nationals, whether business or personal and regardless of where they occur, must be reported to Sandia's counterintelligence office. A security plan is prepared for each foreign national employed by or visiting Sandia that must document the specific physical and cyber access that is authorized. These security plans are reviewed by subject-matter experts from Sandia's physical security, cyber security, counterintelligence, export control, classification, and operational security organizations before approval by the appropriate Sandia vice president. Foreign nationals who are citizens of or were born in countries on the DOE sensitive country list are subject to special scrutiny. Any indication

of behavior beyond that which is authorized is a matter of special security and counterintelligence attention.

Access to classified information requires the appropriate level U.S. Government security clearance and a valid need-to-know. Access to export-controlled information is permitted only if a foreign national has legal permanent residency and a valid need-to-know. Access to other unclassified controlled information, including personal identity information, is also limited by need-to-know.

Employment as a regular Sandia employee is restricted by Sandia policy to individuals who are eligible for a U.S. Government security clearance, which generally means United States citizens. Exceptionally talented foreign nationals who are committed to becoming U.S. citizens may be hired as regular Sandia employees upon completion of a counterintelligence investigation.

The 2008 DOE inspection of Sandia's counterintelligence program lauded the excellent and mutually beneficial relations that exist at Sandia between counterintelligence and both cyber and physical security. The close involvement of counterintelligence with security is essential for strengthening protections against the insider threat.

Assurance is a crucial component of our security program because it engages line organizations directly in security improvement. Self-assessments, a key component of our assurance program, are completed on an annual schedule in accordance with requirements in the relevant DOE directives and are conducted with the assistance of qualified personnel. Self-assessment results are analyzed and trended in Quarterly Management Assurance Reports incorporated in Sandia's Integrated Laboratory Management System. A formal process ensues to conduct causal analyses and risk assessments and to design corrective actions. A verification process exists to track and enable the successful resolution of deficiencies, making sure that corrective actions are completed effectively and are properly documented. The sustainability of corrective actions is also verified during the subsequent yearly self-assessments.

Cyber Security

Sandia National Laboratories has three cyber environments:

- The Sandia Classified Environment (often referred to as “red”) processes secret data of various categories and levels. It uses a separate infrastructure than that of our unclassified networks. Thus, Sandia’s classified information systems are insulated from Internet attacks. The classified environment employs NSA-approved Type-1 encryption on dedicated lines for communication with approved DOE nodes.
- The Internal Restricted Environment (“yellow”) stores all categories of unclassified information, including unclassified controlled information—for example, human resources information, project management data, export controlled information, and proprietary data. Controlled information is protected on a need-to-know basis by access control lists and other technical controls.
- The External Collaborative Environment (“green”) is authorized to store non-sensitive unclassified information but is not authorized to store sensitive information unless additional technical controls are in place, such as encryption.

The yellow and green network environments both connect to the Internet and employ the same protective measures against Internet attacks.

All three environments are centrally managed and controlled. Thus we are able to technically enforce standards on all computers. Sandia’s Network Information System stores data on every machine connected to our networks and is an enforcement tool for ensuring compliance across the laboratory.

Sandia’s information networks and systems are certified and accredited in accordance with NNSA’s Program Cyber Security Plan, which provides specific security requirements for information systems. All Sandia networks and systems are certified by Sandia’s Cyber Security Site Manager and accredited by the NNSA Designated Authorizing Authority.

The “DOE Office of Independent Oversight Cyber Security Inspection” in August 2007 resulted in ten findings, and corrective actions were structured among 26 milestones. We are on track to complete all milestones.

Our unclassified computing environments (green and yellow) are attacked relentlessly. On a typical day, they are bombarded with a quarter million questionable events; after filtering and analysis, tens of thousands of those are established as malicious. Fictional networks that we set

up as targets attract thousands of probes, and we see increasing ingenuity in their design. We typically block 80 percent of the e-mail messages that come to us via the Internet; 92 percent of it is spam, the remainder is malicious email, and much is infected with viruses. Several cyber attempts each day meet the criteria for reportable events to DOE.

Sandia has taken many steps to improve cyber security in response to increased threats. Two-factor authentication is now required for e-mail or access to Sandia's Internal Restricted Environment (yellow) from remote locations. We have augmented commercial e-mail filtering to block malicious software (malware) and deployed technology to identify malicious internet sites that are counterfeit or deceptive. Sandia is aggressively implementing NNSA's diskless classified computing initiative, which includes blocking USB ports and substituting diskless workstation in place of personal computers on classified networks. This initiative will be complete by the end of September.

Sandia's computer security systems isolate cyber attacks and permit our experts to analyze intrusions quickly. Computers identified as possibly engaging in suspicious activity are forensically analyzed and, when necessary, taken off-line for advanced analysis. Appropriate actions are taken to ensure that other systems are not impacted by similar attacks or vulnerabilities. Affected users are notified, and computer system managers are continuously informed of current threats. The results of our forensic analysis are shared with other NNSA laboratories, defense community entities, and law enforcement.

Sandia has completed steps for accreditation of its node of the NNSA Enterprise Secure Network (ESN). ESN will provide a secure capability for classified electronic access among NNSA sites. Sandia had substantial input into the development of the ESN architecture and was the primary contributor to the ESN security plan.

Our strategy for cyber security is designed to engage users in doing a better job of protecting unclassified information, since attacks via the Internet do have the potential to access controlled information. Our internal security management teams continuously assess the evolving risks and threats to our networks and proactively upgrade our defenses with new tools and processes.

We are elevating our focus on the insider threat. Need-to-know controls are in place to protect unclassified controlled information. Upon logging-in to any Sandia network, the user is informed and must acknowledge that he has no expectation of privacy on his usage and that

everything he does on a government-owned computer system is subject to monitoring. And we do in fact monitor. We capture all transactions with the Internet from and to Sandia computers and subject that data to automated analysis for suspicious behavior. E-mails sent from a Sandia account to a foreign address are of special counterintelligence interest. To detect malicious insider activity, we often install software “trip wires” that alert us to unusual behavior. All privileged access (system administrators, database administrators, etc.) are required to use two-factor authentication.

I believe Sandia National Laboratories’ cyber security program is among the most effective in the federal government. However, notwithstanding all the measures we take to protect our unclassified computing environments (both green and yellow), I acknowledge that penetration may occur despite our best efforts. Therefore, we evaluate that risk against the benefit of providing an unclassified computing environment that permits us to conduct laboratory operations in a modern, cost-effective way. We protect controlled content at a high level, and we assure that no content exists in our unclassified environment that could compromise our nation’s nuclear deterrent or security if captured. Consequently, it is my opinion that the security measures on our unclassified computing environments provide an appropriate balance between protection and productivity.

Security Improvement Initiatives

Management at Sandia has strived to go beyond compliance as the main objective and to achieve a security program that is driven by performance goals. We have several initiatives in progress that bring focus to targeted issues where improvement is needed. In March 2007 we kicked off our initiative to review the security footprint at Sandia sites, followed in April by our campaign to reduce classified holdings—both consistent with mission needs. In September 2007 we ordered the lab-wide conversion to diskless workstations on classified networks; in the same month we initiated the rejustification program for vault-type rooms. We also have ongoing programs to improve corporate root-cause analysis, classification awareness, and control of prohibited articles.

On May 15, 2008, I received a letter from the director of the Office of Enforcement at the DOE Office of Health, Safety, and Security. Although the letter was not a formal

enforcement action, it raised concerns about the number of security incidents across DOE sites. The Office of Enforcement's concerns are valid, and we are taking deliberate action to address these concerns.

Based on the concerns expressed in the enforcement letter, we have initiated a lab-wide Security Performance Improvement Project (SPIP) to identify the underlying causes for the continuing security incidents and identify actions that will prevent or mitigate future incidents. Six teams were established to develop specific improvement actions in the following areas: management systems, classified e-mail on unclassified systems, protection of classified files on servers, protection of classified matter, introduction of controlled articles (especially cell phones) to secure areas, and accountability. All teams have completed initial assessments and evaluated root causes. Due to the nature of many of the security incidents, human factors experts are engaged with each team.

I have involved Sandia's senior management in this effort. The laboratory leadership team completed a case study exercise to identify actions within each corporate division that will further reduce incidents, including setting corporate reduction targets for security incidents by division. I require division vice presidents to identify actions and best practices that will help achieve the objectives of this project. Divisions will document their actions and progress in their quarterly Management Assurance Reports.

The power of modern communication technology and computer hardware have challenged security programs across the federal government as never before. We used to think of security as something that could be managed well with robust physical controls. In past decades that was largely true. But today the balance has shifted and the risk is greater on the cyber side than the physical side.

Unfortunately, the balance of resources between physical and cyber security has not been adequately adjusted to reflect that shift, in my opinion. We have done much to reduce the costs of physical security—by removing special nuclear materials, reducing classified holdings, and managing our security footprint, for example—and I believe we can live with a leaner posture for physical security. But to provide security against increasingly sophisticated attacks, cyber defense needs more resources. I was not surprised to learn that Deputy Secretary of Defense Gordon England sent a request to Congress in July asking to shift resources to computer security.

This is an issue that federal agencies are beginning to realize requires more emphasis.

Addressing the Cyber Security Challenge

The cyber threat is a national problem affecting information systems in government as well as the private sector. Given the importance of cyber security to the NNSA complex and the nation, Sandia is actively engaged in understanding the threat and developing technology, systems, and expertise to counter these threats, not only for Sandia, but also for DOE and other national security institutions.

Sandia's growing role in national cyber defense is consistent with its historic mission responsibilities in security systems research and development for DOE and other agencies. We are the design agent for all elements of DOE's transportation safeguards system, a responsibility for Sandia since the 1970s. Similarly, we have partnered with elements of the Department of Defense for decades to develop advanced security technologies for nuclear weapons throughout their life cycle. Our security expertise also contributes to international programs to improve nuclear materials protection and discourage proliferation. In recent years Sandia's programmatic security work has increasingly involved cyber defense, largely because federal missions and civil infrastructures now depend heavily on computer-based systems. Consequently, our research organizations have developed an institutional capability to detect cyber vulnerabilities and to mitigate them.

In September 2007, Sandia worked with DOE to organize the first DOE Summit Conference on Cyber Security. The event stimulated dialog among key stakeholders in DOE on the cyber threat and began the process of developing a broader strategy for cyber-related security issues. It became clear that the NNSA laboratories possess expertise that is highly relevant to this national problem. Subsequently, Sandia supported DOE in a second Cyber Security Summit which allowed the insights and learning derived from efforts started in the first Summit to be shared across a larger set of DOE's organizations.

Sandia's experience in cyber security is a resource for DOE and its laboratories and across many sites. We have worked hard to develop strong teaming relationships across the DOE Complex. Our forensic analysis, incident remediation, and response capabilities are sought out from throughout the complex, as evidenced by requests to assist other sites. Sandia led a tri-lab

simulation exercise in February to model a major cyber security incident involving multiple sites. The simulation demonstrated the incident-response approach that each site applies against cyber attacks and revealed clear benefits of collaboration. Sharing information, resources, and expertise will positively impact the incident-response efforts for participating sites.

Long-term success against the cyber threat will require a steady flow of highly skilled cyber security experts. We recognized some time ago that there were not enough of these people in the pipeline to give us assurance that those skills will be available as today's experts retire. Since 1998 we have offered a "Cyber Defenders" internship program in collaboration with local universities. The mentors and staff of the Cyber Defenders program provide students with cutting-edge research projects while instilling them with new skills. Sandia's Center for Cyber Defenders currently employs nearly 20 students who represent some of the most knowledgeable and passionate students in their field.

The national cyber threat is complex and touches multiple government agencies. It should be addressed through an integrated, government-wide response. I believe Sandia and the DOE laboratories can contribute significantly to the government-wide effort.

Concluding Remarks

Sandia has a longstanding culture of respect for security that is fundamental to our mission. We strive to comply with all applicable directives and requirements, with compliance as the essential baseline from which we advance our security performance. The security program at Sandia is structured with clearly stated lines of authority, responsibility, and accountability. We have done much to reduce the costs of physical security—by removing special nuclear materials, reducing classified holdings, managing our security footprint, and other initiatives. Sandia and its sister laboratories in DOE face a full spectrum of threats from multiple sources and encompassing multiple avenues of attack. The cyber security threat to the nation is especially difficult to manage, and it will require a concerted national response.

WITNESS DISCLOSURE INFORMATION

Witness name: Thomas O. Hunter

Capacity in which appearing: Representative of a government-owned, contractor-operated entity

Name of entity being represented: Sandia National Laboratories

Position held: President and Director

Parent organization (management and operating contractor): Lockheed Martin Corporation

Federal contract: Management and operating contract between Sandia Corporation and U.S. Department of Energy, DE-AC04-94AL85000.

FY2006 cost: \$2,302,377,109; negotiated fee: \$24,306,799

FY2007 cost: \$2,411,647,000; negotiated fee: \$23,214,830

FY2008 estimated cost: \$2,313,723,190; estimated fee: *up to* \$25,142,810

Curriculum Vitae:

Dr. Thomas (Tom) O. Hunter is director of Sandia National Laboratories, with principal sites in Albuquerque, New Mexico, and Livermore, California. Dr. Hunter joined Sandia in 1967 and became president and director in April 2005.

Before assuming his role as director, Dr. Hunter was the senior vice president for defense programs. His management role included oversight of research programs in microelectronics, materials science, engineering science, computer science, and pulsed power; nuclear weapon engineering; information systems and technology; and production and manufacturing. He also had responsibility for the Laboratories' effort in advanced computing, computational science, environmental testing, corporate information systems, and systems integration.

From October 1995 to March 1999, Hunter served as vice president of Sandia's California laboratory. Responsibilities included managing programs in nuclear weapon research and development, nonproliferation, advanced manufacturing technology, information systems, environmental technology, and energy research. He also served as corporate leader for the development of nonproliferation, arms control, and materials management programs.

Earlier in his Sandia career, Dr. Hunter directed Sandia's activities in energy development and environmental quality and emphasized international energy and environment development and supporting information systems. Hunter had a leadership role in establishing cooperative programs in the former Soviet Union to support nonproliferation. He also directed Sandia's nuclear waste management and transportation programs and activities for the Yucca Mountain Project and the Waste Isolation Pilot Plant.

Dr. Hunter is a member of the Engineering Advisory Board for the University of Florida, Council on Foreign Relations, American Nuclear Society, and the U.S. Strategic Command's Strategic Advisory Group. He has served as a member and chair of the Board of Visitors for the dean of the College of Engineering at the University of California, Davis, on various review groups with other Department of Energy laboratories, guest lecturer at Massachusetts Institute of Technology on nuclear waste management, and as an adjunct professor at the University of New Mexico. He is the author of numerous technical papers and presentations. He is a recipient of the 2007 New Mexico Distinguished Public Service Award.

Dr. Hunter earned a bachelor of science degree in mechanical engineering from the University of Florida, a master of science degree in mechanical engineering from the University of New Mexico, and master's and Ph.D. degrees in nuclear engineering from the University of Wisconsin.