Statement of Dr. Samuel G. Varnado
Sandia National Laboratories

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

July 9, 2002

Statement of Dr. Samuel G. Varnado
Sandia National Laboratories

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
July 9, 2002

SUMMARY OF MAJOR POINTS

- Sandia National Laboratories is a multiprogram laboratory operated for the National Nuclear Security Administration (NNSA) of the Department of Energy.
- Sandia and the other NNSA laboratories have technical capabilities that can rapidly accelerate homeland security initiatives.
- We have already made significant contributions in critical infrastructure protection, sensor systems for chem/bio, radiological, and explosive materials; decontamination technology; and nonproliferation systems.
- In anticipation of national needs, Sandia has been investing its LDRD and other appropriate sponsor-provided funds into technologies that have direct application to homeland security and infrastructure protection.
- As a result of our traditional missions and this anticipatory R&D, Sandia has strengths and a growing base of experience in physical security, cyber security, and modeling and simulation that can help protect the nation's increasingly complex and interdependent infrastructures.
- The nation's infrastructure is vulnerable to cyber threats, particularly in the area of Supervisory Control and Data Acquisition (SCADA) systems. As DHS moves forward, these threats should be an area of major focus.
- The proposal to move the National Infrastructure Simulation and Analysis Center, established as a joint program at Sandia and Los Alamos in 2001, is a good one. It will allow NISAC to address national needs and further develop its capabilities in the most effective manner.
- The existing NISAC Joint Program Office should continue to serve as managing entity for NISAC, under the oversight of the new DHS.
- DHS would benefit by establishing a national, multi-agency process to solicit needs and requirements for NISAC.
- Bureaucratic regulations delay and discourage efficient use of the DOE/NNSA laboratories by other agencies. The Homeland Security Act should remove those obstacles to facilitate more direct and agile access by DHS to the capabilities of the national labs.
- Sandia continues its commitment to serve the nation's most pressing national security needs. It is our goal to deliver technology solutions to the most challenging problems threatening peace and freedom.

Statement of Dr. Samuel G. Varnado
Sandia National Laboratories

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
July 9, 2002

INTRODUCTION

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify on the Administration's proposal to create a Department of Homeland Security, and specifically, the critical infrastructure protection activities that will be assigned to the new department. I am Dr. Samuel G. Varnado, Director of Sandia National Laboratories' Infrastructure and Information Systems Center. I have more than thirty-eight years' experience in energy, information, and infrastructure systems development. I currently coordinate the Laboratories' activities in critical infrastructure protection.

Sandia National Laboratories is managed and operated for the National Nuclear Security Administration (NNSA) of the U.S. Department of Energy (DOE) by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation. Sandia's unique role in the nation's nuclear weapons program is the design, development, qualification, and certification of nearly all of the nonnuclear subsystems of nuclear warheads. We perform substantial work in programs closely related to nuclear weapons, including intelligence, non-proliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also conducts research and development for other Federal agencies when our special capabilities can make significant contributions.

At Sandia National Laboratories, we perform scientific and engineering work with a mission in mind—never solely for its own sake. Even the fundamental scientific work that we do (and we do a great deal of it) is strategic for the mission needs of our sponsors. Sandia's management philosophy has always stressed the ultimate linkage of research to application. When someone refers to Sandia as "the nation's premier engineering laboratory," that statement does not tell the whole story: We are a science and engineering laboratory with a focus on developing technical solutions to the most challenging problems that threaten peace and freedom.

My statement, which amplifies my colleague David Nokes' testimony to this committee on June 25, 2002, will describe some of the key problems posed in protecting the nation's critical infrastructure and Sandia National Laboratories' contributions and capabilities in that area. I will also comment on the proposed relationship of that work to the Department of Homeland Security.

SANDIA'S CONTRIBUTIONS TO CRITICAL INFRASTRUCTURE PROTECTION

Like most Americans, the people of Sandia National Laboratories responded to the atrocities of September 11, 2001, with newfound resolve on both a personal and professional level. As a result of our own strategic planning, our LDRD investments, and the foresight of sponsors to invest resources toward critical infrastructure protection, Sandia was in a position to immediately address some urgent needs.

For example, we quickly completed vulnerability assessments of a number of dams in the Western U.S. and worked with the electricity sector to improve the robustness of their supervisory control and data acquisition (SCADA) systems to cyber attacks. These and other contributions to critical infrastructure protection are possible because of strategic planning we had conducted years ago and early investment in the capabilities that were needed to respond. The outstanding technology base supported by NNSA for its core missions is the primary source of this capability. We also made strategic decisions to invest laboratory-directed research and development funds (LDRD) in the very things that we knew were urgent needs: physical security technology, modeling and simulation of infrastructure elements, and cyber security. We were heavily involved in supporting the President's Critical Infrastructure Protection Committee during the Clinton administration, and that activity provided impetus for our current activities. In recent months, requests for Sandia's services from federal agencies other than DOE for work in emerging areas of need have increased. Approximately twenty-eight percent of our total laboratory-operating budget is now provided by federal agencies other than DOE.

SANDIA CAPABILITIES FOR CRITICAL INFRASTRUCTURE PROTECTION

Sandia National Laboratories and the other nuclear weapon laboratories constitute a broad, multidisciplinary technology base in nearly all the physical sciences and engineering disciplines. We leverage those capabilities to support other national security needs germane to our missions, including homeland security, when our capabilities can make significant contributions.

Physical Security

For over 25 years, Sandia has been the lead laboratory for the DOE in safeguards and security. During this time, we have developed risk assessment methodology and used it to design the security approaches for storage and shipment of nuclear weapons and special nuclear material. We have developed vulnerability assessment capabilities and models to optimize mitigation strategies. These models were used in the early days to design protection systems for nuclear power plants as well as for our traditional missions. Recently, the same technology has been used to assess the vulnerabilities and improve the robustness of dams, chemical plants, water systems, conventional electric power plants, and pipelines.

We have developed numerous airport security sensors and systems, including design of secure portals and explosives detectors. Today, a commercially produced, walk-through portal for detecting trace amounts of explosive compounds on a person is available for purchase and installation at airports and other public facilities. The technology for this device was developed, prototyped, and demonstrated by Sandia National Laboratories over a period of several years and licensed to Barringer Instruments of Warren, New Jersey, for commercialization and manufacture. The instrument is so sensitive that microscopic quantities of explosive compounds are detected in a few seconds.

Using similar technology, we have developed and successfully tested a prototype vehicle portal that detects minute amounts of common explosives in cars and trucks. Detecting explosives in vehicles is a major concern at airports, military bases, government facilities, and border crossings. The system uses Sandia's patented sample collection and preconcentrator technology that has previously been licensed to Barringer for use in screening airline passengers. The same technology has been incorporated into Sandia's line of "Hound™" portable and hand-held sensors, capable of detecting parts-per-trillion explosives and other compounds. These devices can be of great value to customs and border agents at ports of entry.

Sandia pioneered a tool called Probabilistic Risk Assessment (PRA) to evaluate the risks in high-consequence systems such as nuclear weapons and nuclear power generation plants. We use this tool to assess the risks in critical infrastructure systems such as dams, water utilities, chemical plants, and power plants. Combined with our expertise in security systems for nuclear facilities, we have helped utilities and industrial associations create security assessment methodologies that help owners and operators determine vulnerabilities and identify mitigation

options. Methodologies have been developed for water utilities, chemical storage facilities, dams, power plants, and electrical power transmission systems.

Cyber Security

Sandia has significant ongoing work in the technology areas intended to protect cyber and network resources and the information that resides on such systems. Programs that assess the vulnerabilities associated with these systems are in place for our own resources as well as for those at other federal government agencies. We conduct red-teaming to challenge information systems and identify and remove vulnerabilities. Our objectives are to enhance the robustness of critical information systems and develop solutions for survivability and response options for systems under attack. Sandia operates a supervisory control and data acquisition (SCADA) laboratory to study the real-time control systems that are used to control the power grid, the pipelines, transportation systems, and water systems. Sandia's capabilities in cyber security arise from our nuclear weapons mission, in which we design the cryptographic systems needed for secure command and control systems for the nuclear stockpile. Sandia is the only DOE laboratory that is approved by NSA to conduct cryptographic research. We have helped many infrastructure owners perform vulnerability assessments and develop risk mitigation strategies.

Modeling and Simulation

National security and the quality of life in the United States rely on the continuous, reliable operation of a complex set of interdependent infrastructures: electric power, oil and gas, transportation, water, communications, banking and finance, emergency services, law enforcement, government continuity, agriculture, health services, and others. Today, these systems depend heavily on one another; that interdependency is increasing. Disruptions in any one of them could jeopardize the continued operation of the entire infrastructure system. Many of these systems are known to be vulnerable to physical and cyber threats and to failures induced by system complexity.

In the past, the nation's critical infrastructures operated fairly independently. Today, however, they are increasingly linked, automated, and interdependent. What previously would have been an isolated failure could cascade into a widespread, crippling, multi-infrastructure disruption today. Currently, there are no tools that allow understanding of the operation of this

complex, interdependent system. This makes it difficult to identify critical nodes, determine the consequences of outages, and develop optimized mitigation strategies.

The National Infrastructure Simulation and Analysis Center (NISAC) concept, which would be transferred to the Department of Homeland Security under the Administration's bill, is also an example of our experience with critical infrastructures and will be described and discussed later in this statement.

CRITICAL INFRASTRUCTURE PROTECTION PROBLEMS

The U.S. infrastructure is difficult to protect because of its size and complexity. There are many avenues for possible exploitation by an adversary. In this statement, I will address two of the problems we consider to be the most serious.

Cyber Security

Computerized supervisory control and data acquisition (SCADA) systems control the operations of critical infrastructures such as power utilities, distribution networks, and municipal water supplies. These systems have generally been designed and installed with little attention to security. They are highly vulnerable to cyber attack. In fact, it has been claimed that it is possible to turn the lights off in many major cities with a cyber attack. An article in the June 27, 2002, edition of the *Washington Post* adds credence to this claim, and states that these systems have been the targets of probing by Al Qaeda terrorists. Some government experts conclude that the terrorists plan to use the internet as an instrument of bloodshed by attacking the juncture of cyber systems and the physical systems they control. The article further postulates that combined cyber and physical attacks could generate nightmare consequences.

Sandia has been investigating vulnerabilities in SCADA systems for five years. During this time, many have been found. Our assessments show that security implementations are, in many cases, non-existent or based on false premises. Some of the vulnerabilities in legacy SCADA systems include inadequate password policies and security administration, no data protection mechanisms, and information links that are prone to snooping, interruption, and interception. When firewalls are used, they are sometimes not adequately configured, and there is often "back-door" access because of connections to contractors and maintenance staff. We have found many cases in which there is unprotected remote access that circumvents the firewall. From a security perspective, it should be noted that most of the SCADA manufacturers are foreign-owned. In

summary, it is possible to covertly and easily take over control of one of these systems and cause disruptions with significant consequences. Recognition of that fact led numerous federal agencies and municipal water and transportation systems to request Sandia help following September 11.

Of even more concern is the fact that the control systems are now evolving to the use of the internet as the control backbone. The electric power grid is now, under restructuring, being operated in a way for which it was never designed. More access to control systems is being granted to more users; there is more demand for real time control; and business and control systems are being connected. Typically, these new systems are not designed with security in mind. More vulnerabilities are being found, and consequences of disruptions are increasing rapidly. Industry is now asking for our help in understanding vulnerabilities, consequences, and mitigation strategies. After September 11, Sandia also received requests for help from private companies and professional societies.

Interdependencies

The U.S. infrastructure is becoming increasingly interdependent. For example, the banking and finance sector depends upon telecommunications, which depends on electricity, which depends on coal, gas, oil, nuclear sources, water, and transportation. These interdependencies create the potential for high consequence, cascading failures in which a failure in one element of the infrastructure leads to failures in others. Further, interdependencies make it difficult to identify critical nodes, vulnerabilities, and optimized mitigation strategies. We have studied one case, for example, in which the best way to assure operation of the electric power grid is to protect the gas pipeline that feeds the generation stations in that area. The bottom line is that interdependencies cause the infrastructure to behave as a complex system whose behavior is difficult to predict.

Most of the current federal critical infrastructure protection activities are directed at individual infrastructure elements. This stovepiped approach was reinforced by PDD-63, in which various agencies were assigned responsibility for protecting specific infrastructure elements (e.g., DOE was assigned electricity and oil and gas, DOT was assigned transportation, etc.). While it is necessary to understand these individual elements, the more compelling problem is to address the interdependent nature of the behavior of the infrastructure in order to prevent more severe consequences. We believe that this modeling and simulation effort is

essential and will lead to the ability to define the critical nodes at the system level, identify consequences of outages, and define optimized protection strategies.

POSSIBLE SOLUTIONS TO CRITICAL INFRASTRUCTURE PROBLEMS

It is unreasonable to expect that every part of the infrastructure can be completely protected. Rather, a risk management strategy must be used to decide where to invest limited protection resources. Three steps are needed:

- Define the infrastructure elements that are truly critical. Criteria must be established that define "critical". These could include, for example, loss of life, economic impact, time to rebuild, cost to rebuild, potential for loss of confidence in the government, etc.
- Perform vulnerability assessments for these critical elements.
- Develop optimized prevention and mitigation strategies.

It will be necessary to work closely with private industry in all these steps, since they own 85% of the US infrastructure. They must see a business case, based on risk analysis, before they are willing to invest in protection. Vulnerability assessment methodology is well known to Sandia, other DOE labs, and certain private companies. They can play important roles in all three steps, but especially in identifying, from a systems perspective, the critical nodes and in evaluating the consequences of disruptions so that business cases can be developed. The methodology for conducting the required analysis is known. What is needed from a technology development perspective is additional research in cyber security techniques and development of additional simulation and modeling capability, since modeling of the behavior of complex systems will require high performance computing. Additionally, help is needed in working with private industry. Many of the private owners of the infrastructure feel that identification of critical nodes and vulnerabilities is sensitive information, and they are reluctant to share it with the government. Government action is needed to create a process under which sensitive information can be shared among those in government and industry with a need-to-know.

Congressional support is needed to help implement the following steps that will lead to a more robust national infrastructure:

- Establish a new category of sensitive, restricted information for Critical Infrastructure Protection applications. Procedures for protecting the information and processes for granting access to both industry and government personnel are needed.

- Provide training in vulnerability and risk assessment methodology to private industry.
- Support additional research into cyber security issues, including cryptographic methods such as authentication, low power encryption methods, and standards. The establishment of test beds to allow evaluation of competing technologies should be encouraged.
- Support development of tools needed for identifying critical nodes, consequences of outages, and optimized mitigation strategies.

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER (NISAC)

The President's bill to establish a Department of Homeland Security provides for an Under Secretary for Information Analysis and Infrastructure Protection. It further proposes, under Title II, to transfer the responsibility for NISAC to the Department of Homeland Security. NISAC was formally chartered by the USA Patriot Act of 2001 (Oct 26, 2001) to serve as "a source of national competence to address critical infrastructure protection and continuity through support for activities related to counter terrorism, threat assessment, and risk mitigation." (Section 1016 of Public Law 107-56, the USA Patriot Act, 10/26/2001). NISAC, a partnership of Sandia and Los Alamos national laboratories, is leveraging current modeling, simulation, and analysis expertise to develop higher fidelity simulations crucial to the success of the Nation's critical infrastructure protection program. These labs were chosen to manage NISAC because of their considerable investment in infrastructure and interdependencies modeling over the last decade, the availability of high performance computers at the labs, and their modeling and simulation capabilities.

Status

The President's FY03 budget request called for the FY03 NISAC activities to be funded through the Department of Energy. NISAC, with Sandia and Los Alamos national laboratories as core partners, has devoted considerable effort to expanding the critical infrastructure modeling, simulation, and analysis capabilities of the two laboratories. A Joint Program Director has been selected to manage the NISAC program on behalf of both labs. NISAC has built consensus in the government and private sector on the importance of infrastructure interdependency analysis to the nation's critical infrastructure protection program. The NISAC Joint Program Office is developing strategic plans and associated research and development programs to meet its national charter. These plans include the identification of key strategic

partners from other labs, universities, and private industry who will serve as technical collaborators in the performance of the tasks assigned to NISAC. Further, NISAC has proposed a senior-level, national, interagency process, including DHS, to generate, prioritize, and set national-level requirements for its modeling and simulation activities.

Observations

The proposal to move NISAC to the Department of Homeland Security is sound. It will allow NISAC to serve as a national resource that can address critical infrastructures and, most importantly, their *interdependencies* across the entire range of infrastructure elements – energy, telecommunications, transportation, banking and finance, water, etc. It will allow the NISAC work to be prioritized by national needs, rather than the by the interests of a single agency. Further, it will be possible to implement a national level requirements-setting process for NISAC activities, which fulfills the intent of the Patriot Act.

It is important that the existing NISAC Joint Program Office continue to serve as the managing entity for NISAC, serving under the oversight of the new DHS, in order to capitalize on the previous decade's investment in the technology base. An added benefit to the proposed organizational structure within DHS is that it would place NISAC and the National Communications System (NCS) under the same Under Secretary. NCS has significant capability in modeling the telecommunications infrastructure, while Sandia and Los Alamos have similar capabilities in modeling the energy infrastructure, chem./bio problems, and infrastructure interdependencies. This concentration of technical capability in one organization will provide a demonstrated competence that should lead to early and useful results.

Recommendations

- The legislation that establishes the Department of Homeland Security should clearly state that NISAC will be managed by the NISAC Joint Program Office for the Department of Homeland Security.
- The legislation should state that DHS will assume both funding and oversight responsibilities for NISAC as soon as DHS is established. A NISAC program manager within DHS should be named.
- The Homeland Security Act should give the Department of Homeland Security the power to task the NNSA laboratories directly, just as do the Science, Energy, Environmental, and

other non-NNSA offices of DOE. That authority would eliminate the bureaucratic red tape and additional costs associated with the Work-for-Others (WFO) process.

- The legislation should require that DHS establish a national level, multi-agency process to solicit needs and define requirements for NISAC. Participating agencies could include DOE, DOT, DOC, OSTP, DOS, Treasury, and others. Final approval for all NISAC activities should reside with a senior DHS official.

SUMMARY AND CONCLUSION

Sandia National Laboratories and the other NNSA laboratories constitute a broad, multidisciplinary technology base in nearly all of the physical sciences and engineering disciplines. We are eager to leverage those capabilities to support the science and technology needs of the Department of Homeland Security when our capabilities can make significant contributions.

Sandia possesses strong competencies in physical and cyber security and in modeling and simulation. Most of this technology is suitable for transfer to industry and deployment in homeland security applications. We have been proactive in addressing the challenges of infrastructure protection. We have a track record of anticipating emerging homeland security threats and investing in technology development to counter them through our Laboratory-Directed Research and Development program and sponsor-directed programs. We are one of the premier laboratories for working with industry to transform laboratory technologies into deployable commercial applications. Bureaucratic and regulatory roadblocks exist that limit access to the DOE/NNSA national laboratories by other federal agencies, and those obstacles should be removed by the homeland security legislation in order to facilitate direct access to those resources.

On behalf of the dedicated and talented people who constitute Sandia National Laboratories, I want to emphasize our commitment to strengthening United States security and combating the threat to our nation's critical infrastructures. It is our highest goal to be a national laboratory that delivers technology solutions to the most challenging problems that threaten peace and freedom. Thank you, Mr. Chairman. I would be pleased to respond to any questions you may have.

WITNESS DISCLOSURE INFORMATION

Witness name: Samuel G. Varnado

Capacity in which appearing: Representative of a non-government entity

Name of entity being represented: Sandia National Laboratories (GOCO)

Position held: Director, Infrastructure and Information Systems

Parent organization (managing contractor): Lockheed Martin Corporation

Federal contract: Management and operating contract between Sandia Corporation and U.S. Department of Energy, DE-AC04-94AL85000.
FY2000 cost: $1,540,019,000; negotiated fee: $16,110,000.
FY2001 cost: $1,580,187,000; negotiated fee: $16,300,000.
FY2002 cost: $1,684,552,000; negotiated fee: $17,270,000.

Career biography:

Dr. Varnado is currently Director of the Infrastructure and Information Systems Center at Sandia National Laboratories. In this role, he leads Sandia's Critical Infrastructure Protection Program and manages Sandia's efforts in information surety and defensive information warfare.

Dr. Varnado has a breadth of experience in research, administration, and marketing. He has been at Sandia in a variety of capacities for most of his career. Previously, he held the position of Director of Energy and Critical Infrastructure Technology at Sandia. His earlier activities included coordinating all Sandia's DoD funded programs and management of a systems analysis organization.

He also spent ten years in private industry in research and marketing positions for an oil field service company. His last position, before returning to Sandia in 1990, was as Vice President of Marketing Technology for NL Sperry-Sun in which he had responsibility for worldwide marketing of NL's new measurement-while-drilling systems. He has published extensively in the energy field.

He earned a BS degree from Mississippi State University, an MS degree from the University of New Mexico, and a PhD degree from the University of Texas at Austin, all in electrical engineering.