

Testimony Highlights
Mr. Bradley A. Peterson & Dr. Linda R. Wilbanks
National Nuclear Security Administration
U.S. Department of Energy
Before the
House Committee on Energy & Commerce
Subcommittee on Oversight & Investigations
September 25, 2008

- While the NNSA faces many challenges, and has room to improve, we continue to make enhancements in our physical and cyber security posture that will maintain security at our sites as strong and robust.
- Whether it is the physical or the cyber threat, the first premise on how we protect our most important information is based upon the government-wide processes for the protection of multiple levels of classified information, material and technologies and the application of risk management principles. We utilize a graded security approach, with defense in depth security systems, based on the information and assets at each facility or on each network, and the perceived threat to that facility. Our security is continuously tested and evaluated to expose weak links and areas for improvement.
- NNSA has a robust technical-, operational-, and management-based approach to the cyber security of unclassified, controlled unclassified, and classified information. We believe our approach, which is continually improving, is sound and provides effective security for our unclassified and classified networks. But, the nature of the threat changes daily, and we must maintain the pace of our own advances and continue to improve the collaboration between our sites, DOE, and cyber security experts across the government and industry to succeed in the future.
- NNSA operates some of the most physically secure facilities in the world and generally have maintained effective programs and seen positive improvements in the past two years in the area of physical security at the weapons' laboratories. That said, we face many challenges in consistently maintaining fully effective programs. An exhaustive security planning process, a detailed program development process, and in-depth controls and oversight of the implementation of our programs provide the basis for ensuring security readiness.
- Maintaining highly effective security for nuclear weapons, weapons components, special nuclear material, and classified and sensitive information is our highest priority. In today's post 9/11 environment, especially in the computer age, we will continue to rely on sound, risk-based security principals to guide our physical and cyber approach: the effective separation of classified and unclassified information and computer networks; the strengthening of defensive systems to detect, deter and deny adversaries from entering our networks or removing information; an intelligence based graded security approach to the protection of our sites; and an effective and active training regime and federal contractor oversight program. As holders of some of the most desirable material and information to our enemies, we recognize our enemies will not take a day off, and we cannot either.

**Statement of
Mr. Bradley A. Peterson
Chief, Defense Nuclear Security
& Associate Administrator for Defense Nuclear Security
&
Dr. Linda R. Wilbanks
Chief Information Officer
National Nuclear Security Administration
U.S. Department of Energy
Before the
House Committee on Energy & Commerce
Subcommittee on Oversight & Investigations**

September 25, 2008

Chairman Stupak and members of the subcommittee, we appreciate the opportunity to appear before you today to address an issue that the National Nuclear Security Administration (NNSA) at both our headquarters and our sites consider to be one of our top priorities – security. We appreciate the chance to provide an account of where we are succeeding, where we are making progress, and where we are applying greater focus and effort. We appreciate this subcommittee’s efforts to ensure the nation’s nuclear weapons enterprise retains the highest degree of protection against both physical and cyber threats.

We can assure you today, that while the NNSA faces many challenges, and has room to improve, we continue to make enhancements in our physical and cyber security posture that will maintain security at our sites as strong and robust.

As you can imagine, given the nature of the information, and the material and technology we are responsible for, NNSA’s nuclear facilities face a broad range of potential and real physical and cyber security threats that we protect against on a daily basis. Physically, the threat is similar to what it has always been and ranges from insiders – inadvertent personnel failures,

disgruntled employees, and potential active adversary support – to potentially highly damaging direct external attacks by violent individuals, organized crime, terrorist groups or nation states.

The cyber threats to the Department of Energy (DOE) and NNSA are similar to those faced by the entire U.S. Government, every public and private enterprise, and any individual; essentially, anyone connected to a computer in a free society exposes themselves to potential attack. NNSA facilities are the target of over one million attacks of varying sophistication every day, ranging from relatively harmless curiosity seekers to sophisticated hackers, to corporate thieves, to nation-state and belief-based espionage.

To that end, whether it is the physical or the cyber threat, the first premise on how we protect our most important information is based upon the government-wide processes for the protection of multiple levels of classified information, material and technologies and the application of risk management principles. We utilize a graded security approach, with defense in depth security systems, based on the information and assets at each facility or on each network, and the perceived threat to that facility. Our security is continuously tested and evaluated to expose weak links and areas for improvement. As expected, we do find such issues on occasion. In cyber space, we can say very confidently that our classified networks, which protect the “crown jewels,” are extremely well protected. Our unclassified and controlled unclassified networks face a higher level of risk due to the sophisticated threats we face from our adversaries in cyber space. However, we rely on the subject matter experts in our Classification Program to keep classified information off those networks, and our layered internal and external defenses are designed to deter, detect, and stop as many of these attacks as possible from being

successful. If an attack penetrates one or more layers of our defenses, we have tools to detect, contain the penetration, assess the potential damage, and eliminate the threat.

The Cyber Security Challenge

NNSA takes the responsibility for securing the critical information that resides at our sites very seriously. First and foremost, we operate separate network systems for our classified and unclassified information. Information classified according to Executive Orders, the Atomic Energy Act, and DOE Directives is housed in classified networks which are “air-gapped” from our unclassified and controlled unclassified networks. We have implemented hardware, software, and administrative controls, including personnel training and a “diskless workstation” initiative across the complex to manage the movement of data within the classified networks and control the “air-gap.”

In May 2008, new NNSA policy was issued addressing many recommendations and findings on our classified and unclassified networks. This policy was developed in collaboration with our sites and hence many of the components, such as certification and accreditation and security plans were implemented prior to May. At the Los Alamos National Laboratory (LANL), all networks, classified and unclassified, are being re-certified to ensure they meet the critical security plans and certification and accreditation requirements; all indications are that this will be completed on all networks by the deadline of December 8, 2008.

In addition to the new policy, NNSA, jointly with DOE, is converting by September 30, 2008, over 11,000 Accountable Classified Electronic Media (ACREM) to diskless systems, greatly decreasing the risk of loss. Approximately 2,000 ACREM have received temporary waivers, justified by the site office and validated by Headquarters. NNSA stood up a new classified network in April 2008 to facilitate the exchange of classified data and provide a standardized, secure computing environment that ensures the protection of NNSA information assets, reduces costs, avoids duplication of efforts, improves trust and confidence from management and partners, safeguards the environment, and improves the ability to manage and monitor classified data.

We have many layers of protection and detection for our classified networks that we are pleased to discuss in a classified environment.

Our testimony today is focused primarily on our unclassified networks, what are referred to as the “yellow” networks. Guidelines for unclassified and controlled unclassified information are specified through various Federal authorities, including DOE. We have implemented those guidelines and conduct certification and accreditation of systems and applications to ensure those controls have been implemented as directed and are effective.

Every Federal agency across the U.S. Government, including NNSA and DOE, are under cyber attack every day. Measures to isolate ourselves from the outside world on unclassified matters would be extremely expensive and have a severe negative impact on the ability of NNSA to accomplish its missions, especially as we work to make a smaller nuclear weapons enterprise

that is more efficient and responsive. We acknowledge the need for improvement as detailed in recent Government Accountability Office, DOE Inspector General and DOE Office of Health, Safety and Security (HSS) reports. We are focused on improving controls on our networks to ensure that we have a comprehensive, highly effective security system to address our risks, and to minimize and contain the damage if an attack penetrates our defenses.

In addition to segregating our unclassified networks from the classified networks, we have implemented additional administrative and firewall systems to control access to the data within each unclassified and controlled unclassified network. For example, at each site, Personally Identifiable Information (PII) may only be needed by some people within the respective Human Resources organization and the controls within the network manage access to the data. In addition, our national laboratories have established separate networks for foreign nationals, limiting their access to the information needed to do their jobs.

While we have made significant progress against the cyber threat, as documented in the GAO's recent report, in the not too distant past, LANL had not properly structured their access controls for certain unclassified data, allowing some users access to information that was not required for the performance of their duties. LANL is implementing improved access controls which will strengthen physical and logical network separation to control access to this information.

Other tools we use for cyber protection are multiple firewalls and monitoring systems. These systems manage and check incoming and outgoing traffic to ensure it is authorized and

there are no anomalies. Other systems check electronic traffic inside our networks to ensure that programs and files are authorized to be on our system.

Multiple levels of sensors are also employed to safeguard important information: first, at the site level, where most of the initial detections are made and problems are resolved; second, at the NNSA enterprise level, looking for known or suspected data transfer patterns gleaned from inside information and external Federal sources; and third, national level sensors to help identify suspicious activity. When our systems detect unusual activity we quickly terminate the communications pathways, and when necessary, selectively isolate portions of our networks to quarantine any potentially harmful activity. Once the harmful activity is isolated, we deploy forensic capabilities to eradicate the threat and restore the system to secure operations.

Our unclassified “yellow” networks contain important and sensitive information such as Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), Export Control Information (ECI), and Personally Identifiable Information (PII). In addition to the security protections of the “yellow” networks themselves, we impose additional controls on access and transmission of this type of information including encryption during transmission and in storage, and the use of two-factor authentication for remote access. In some cases, separate physical networks, although not required, have been implemented at NNSA sites to minimize the accessibility of this information. We continue to assess other controls, collaborate with our peers across Government, and leverage the results of assessments to find even better ways to protect our unclassified networks.

NNSA's cyber security program leads DOE in implementing Departmental required controls for unclassified networks, and in many cases has implemented additional technical and administrative controls to provide further protection. We employ exceptional people, we look for enterprise solutions, and we issue clear direction and guidance regarding the controls that are to be implemented and the processes for ensuring those controls are effective. Our labs and plants work extremely hard to maximize their protection levels.

As GAO has indicated, LANL's networks were not as secure as they needed to be last year and Secretary Bodman issued a Compliance Order that directed needed improvements in late 2007. As a result of this, and LANL's work to fulfill the Compliance Order, their cyber security posture has improved greatly. For example, by December 2008, over 50% of the GAO recommendations will have been implemented, with the remainder to be met by December 2009.

Finally, we have established strong and effective cyber security incident response capabilities. This is done through the coordinated efforts of a team of cyber security experts spanning all of our NNSA and DOE locations, including our laboratories. DOE Office of the Chief Information Officer (OCIO) and NNSA have partnered to implement a state-of-the-art Computer Incident Response Capability (CIRC) in Las Vegas, Nevada. The DOE-CIRC monitors DOE and NNSA networks and coordinates the response to incidents by utilizing extensive communications and collaboration among the NNSA and DOE facilities to deter attacks and respond to those attacks that enter our networks. This effort is supported by extensive communications between DOE and NNSA sites, other Federal Agencies, the law enforcement,

intelligence and counter-intelligence communities, and the technical community to understand the current and anticipated threat, and develop state-of-the-art defenses.

In summary, NNSA has a robust technical-, operational-, and management-based approach to the cyber security of unclassified, controlled unclassified, and classified information. We believe our approach, which is continually improving, is sound and provides effective security for our sensitive and classified networks. But, the nature of the threat changes daily, and we must maintain the pace of our own advances and continue to improve the collaboration between our sites, DOE, and cyber security experts across the government and industry to succeed in the future.

The Physical Security Challenge

Unlike cyber security, we are not under daily physical attack at our sites; however, we must maintain a robust security posture coupled with a high level of readiness to ensure we are always prepared for any credible threat, given the potential consequences of a successful physical attack. Our current physical security protection posture has been designed to effectively address the threat planning assumptions outlined in the 2003 Design Basis Threat (DBT) Policy. DOE HSS has replaced the DBT with the recently announced Graded Security Protection (GSP) Policy and we are just starting the process of conducting new vulnerability analyses that will form the technical basis for our physical security protection postures.

Our vulnerability assessment approach will ensure that site protection strategies are sufficient to provide an effective defense against a very wide array of potential attacks, including low probability but high consequence scenarios. The robust threat scenarios that we plan and test against are also the scenarios that are extremely demanding in their need for high levels of preparation and planning by the adversary and, consequently, have the highest potential for pre-attack discovery. Any pre-attack warning can greatly leverage the capabilities of security forces designed to counter such threats.

We operate some of the most physically secure facilities in the world and generally have maintained effective programs and seen positive improvements in the past two years in the area of physical security at the weapons' laboratories. That said, we face many challenges in consistently maintaining fully effective programs. An exhaustive security planning process, a detailed program development process, and in-depth controls and oversight of the implementation of our programs provide the basis for ensuring security readiness. Sometimes, reviews expose shortcomings that raise our awareness of areas where our performance needs to be improved.

For example a routine HSS Independent Oversight assessment of LLNL security programs was conducted in May 2008, including full scale "force-on-force" exercises. The force-on-force exercises involved a tactical security team playing the role of an attacking force in a free play environment. These exercises are an important tool in evaluating security by stressing our protective forces in the areas of command and control, communications, individual and team tactics, and equipment performance. Overall, while the inspection team noted some

positive areas and attributes of the program, the protective force and classified matter protection and control were rated as having “significant weaknesses.” Two other areas, physical security systems and protection program management, were rated as “needs improvement.”

In response to the inspection results, immediate actions to address the most pressing deficiencies were made, including: placing special nuclear material in a more secure storage configuration; curtailing normal operations until the security posture was deemed ready; and adding additional protective force personnel to each shift. Immediately after the inspection, NNSA sent a team of headquarters and field security experts to assess the LLNL response to the inspection. In addition, senior NNSA officials discussed the severity of these security issues with the Lab Director and with the Board of Governors of the Laboratory’s operating company, Lawrence Livermore National Security, LLC to advise them that the results of the security inspection and their response would be factored into their annual contract assessment.

These independent evaluations help identify weakness in our systems so we can continually improve them. While the LLNL protective force was conducting performance tests on individual elements of the overall protection strategy, prior to the HSS inspection they were not conducting larger scale tactical testing, which would have tested the overall protection strategy and identified any shortcomings in putting those tactical pieces together. In addition, the federal oversight at the Site Office and headquarters level was not effective in this area and did not identify the lack of comprehensive testing as an issue in their oversight activities or a shortcoming in the overall program.

This is being addressed at multiple levels since the inspection. LLNL has conducted numerous successful force-on-force exercise and limited scope performance tests. These have resulted in assurances that protective force personnel can effectively execute Security Incident Response Plans, and that they are thoroughly familiar with engagement simulations systems that replicate normal duty weapons and equipment. Equipment malfunctions that hampered performance during the HSS force-on-force exercise have been addressed to provide the required assurance that these systems will be available to support the Laboratory's security response operations. Issues with the mobile weapons platform (MWP), the most significant equipment problem identified, have been analyzed and are being addressed. Repairs and upgrades to the MWP already completed provide confidence that this system will perform reliably and effectively during an emergency. Additional upgrades are planned for the MWP to enhance its performance and endurance.

In addition to monitoring LLNL's progress, we have also focused on ensuring that these same issues do not exist at the other weapons laboratories. The HSS Office of Independent Oversight is currently completing an inspection at LANL that appears to confirm our assessment of the physical and protective forces. The most recent HSS inspection at Sandia National Laboratory-New Mexico identified their physical security and protective forces programs as effective.

We understand the value of effective oversight and are continually working to improve our process, through a "cycle of learning." In 2007, the NNSA Administrator chartered several "Special Focus Area Groups," one of which was organized to improve the Federal line

management oversight of safety and security. As a result of this group's activities, we are preparing to issue a supplemental directive to the Department's oversight policy, detailing how we will manage our oversight activities. In addition, we have implemented an enterprise wide Contractor Assurance System that is critical to ensuring the national laboratories have a robust and comprehensive self-assessment program, which is the first line of defense in identifying security issues.

Ultimately, the key to a successful security program across the NNSA and our weapons laboratories is a comprehensive program that strives to continuously improve, and is continuously subjected to rigorous oversight. We have challenges, but our baseline security infrastructure and programs are effective and improving. A few recent specific recent achievements across our laboratories include:

- Completing the removal of Category I and II Special Nuclear Material from Sandia National Laboratory-New Mexico and re-distributing armored vehicles, weaponry, and ammunition to other sites in the Complex.
- Progressing ahead of schedule, and utilizing all available shipping capacity, to eliminate Category I and II Special Nuclear Material from LLNL by 2012.
- Adding additional barriers and weapons systems, and enhancing nuclear material vaults.

- Upgrading the vault-type rooms (VTRs) to improve the protection of classified matter.

- Conducting many more limited-scope training exercises and force on force exercises to improve protective force command and control, communication, protective force response tactics and physical security.

- Reducing our classified footprint at sites like LANL.

Notwithstanding these improvements, both DOE and GAO auditors have highlighted areas at LANL where we must devote additional attention and resources. The GAO in particular is concerned with our ability to sustain the improvements made at LANL and identified the need for us to have a better strategic plan. Given the history at Los Alamos it is hard to disagree with those concerns and the recommendation. We have recently hired a new Federal security manager for the site and my office will be working closely with him and his staff to build a strong security program at Los Alamos and address these issues. As the GAO and DOE auditors point out – there is a strong foundation of improvements to build from, the key of course is sustainment of the security improvements, this will continue to be a primary objective for NNSA in the coming years.

Summary

In closing, maintaining highly effective security for nuclear weapons, weapons components, special nuclear material, and classified and sensitive information is our highest priority. In today's post 9/11 environment, especially in the computer age, we will continue to rely on sound, risk-based security principals to guide our physical and cyber approach: the effective separation of classified and unclassified information and computer networks; the strengthening of defensive systems to detect, deter and deny adversaries from entering our networks or removing information; an intelligence-based graded security approach to the protection of our sites; and an effective and active training regime and federal contractor oversight program. As holders of some of the most desirable material and information to our enemies, we recognize our enemies will not take a day off, and we cannot either.

This concludes our formal remarks, and at this time we would be pleased to answer any of your questions.