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

September 25, 2008

Mr. Chairman and members of the subcommittee, thank you for inviting me to testify today as you seek information on the status of the safeguards and security and cyber security programs at the National Nuclear Security Administration's (NNSA) three national weapons laboratories: Los Alamos, Lawrence Livermore, and Sandia. As the Department's Chief Health, Safety and Security Officer, I have a direct interest in the levels of rigor and effectiveness with which the laboratories implement the Department's security policies and requirements.

Office of Health, Safety and Security Responsibilities

In addition to its responsibilities in the areas of environment, safety, and health, the Office of Health, Safety and Security (HSS) is directly responsible for the corporate level elements of the Department's safeguards and security programs. With the exception of cyber security policy, which falls under the purview of the Department's Chief Information Officer, HSS develops and promulgates safeguards and security strategies, policies, and policy guidance that establishes the standards for the protection of Departmental assets. HSS also provides technical assistance to program offices and field sites in implementing those policies; and conducts independent oversight of safeguards and security and cyber security programs throughout the Department. It

is through the results of our independent oversight activities that I can directly address your areas of interest today by describing our assessment of the current performance of the weapons laboratories in implementing programs to protect special nuclear materials, classified matter, and cyber assets. Due to the unclassified nature of this hearing, I can only address problem areas in general terms, but I can nevertheless provide a bottom line regarding the adequacy of protection.

Protection of Special Nuclear Materials

Among the assets in the custody of our weapons laboratories, special nuclear materials are among our most sensitive national security assets and are afforded very high levels of protection. I can tell you with confidence, based on analyses of our most recent independent oversight evaluations and subsequent information, that all three laboratories are adequately protecting these materials.

That is not to suggest that the highly complex protection systems at the laboratories are without deficiencies. For example, some problems were identified in the area of material control and accountability at Los Alamos and, earlier this year performance testing at Lawrence Livermore revealed that although the protective force was well equipped and well trained in the necessary individual skills, they experienced key equipment malfunctions and some difficulty in implementing response actions required to execute a fully effective tactical response. In this specific instance, NNSA and laboratory management responded quickly to implement compensatory measures to address these shortcomings. To date, reports of progress indicate that

they are aggressively addressing identified deficiencies; however, we will be unable to validate such progress until we return next spring to assess the effectiveness of site corrective actions.

Protection of Classified Matter

The weapons laboratories, by virtue of the nature of the business they are in, generate, receive, manipulate, and store large quantities of classified matter. Unlike nuclear materials, which are confined to a small number of locations and accessible to relatively few employees, classified matter is generally dispersed among many locations throughout the laboratories and the majority of the employee populations may be involved to varying degrees in its use and protection. Results of our evaluations indicate that the systems in place to protect classified matter at the weapons laboratories are generally adequate and in compliance with expectations, but there are residual issues that must be addressed to further improve various aspects of the protection systems. For example, in our most recent inspections of the laboratories, we have identified problems with alarm sensor coverage in a small percentage of vault-type rooms; longstanding dependence on the use of non-standard storage for classified parts; recurring problems with the proper control and accountability of classified removable electronic media; and weaknesses in management and storage of classified documents. Often we find problems such as these to be isolated in nature, such as a few of perhaps hundreds of accounts/storage locations at a laboratory. While isolated mistakes can be expected considering the magnitude of this task, there remains the need for sustained, and in some cases increased effort in this area.

Cyber Security

Finally, let me address another area involving information security, and one in which I believe the members of the subcommittee have a particular interest. Threats to DOE and NNSA cyber security defenses are rapidly escalating both in terms of the number of attacks and in the sophistication and complexity of those attacks. This environment makes it particularly challenging to produce and implement improvements in Departmental policies, procedures, and technical solutions in a manner that keeps pace with the constantly evolving threat.

Classified Cyber Security

I would like to begin by outlining the progress and challenges associated with classified cyber security programs at our weapons labs. Our independent oversight inspections have identified several positive attributes of the classified cyber security programs at each of the weapons laboratories. These include the segmentation of computer networks to improve need-to-know protection controls, improved vulnerability scanning and patching processes, and the move toward centralization of management responsibilities for most information systems. Additionally, the near completion of the diskless workstation task force project has resulted in the conversion of the vast majority of classified workstations within DOE and NNSA to "diskless" operation, where there is no local disk drive and therefore classified information is stored on secured servers. This effort has significantly reduced the risk of losing classified information through intentional or unintentional mishandling of classified electronic media.

However, while progress has been evident in many areas, individual laboratory cyber security policies and procedures are not uniformly comprehensive and all are not yet up to date with recently issued DOE and NNSA requirements. Additionally, comprehensive documentation of all of the current technologies and risk mitigation strategies implemented at a particular laboratory is often missing. And, for those systems and networks that are not centrally managed by the weapons laboratories' central information technology groups, but instead are managed by individual research divisions, our technical testing and programmatic reviews show that many of these systems are not consistently kept up to date with security patches and that secure configurations are not always implemented or enforced.

Another example where processes are not fully mature is in the area of certification and accreditation of classified information systems. Although sites have deployed generally good configuration management programs, their processes do not always include the technical means to validate that security controls remain in place once a system is deployed, essentially invalidating the original basis for acceptance of the remaining risks. In addition, because security plans do not always address all aspects of the accreditation boundaries, the associated security tests do not examine all of the systems on those networks to ensure that controls are effectively implemented.

Many of the problems noted above can be partially attributed to longstanding gaps and weaknesses in cyber security policy. Both DOE and National cyber security policy have been in a state of flux for several years and cyber security performance across the Department has suffered as a result. That said, I would like to acknowledge that the DOE Office of the Chief

Information Officer recently issued new cyber security policy for national security systems and the Office of the NNSA Chief Information Officer followed with an updated threat statement and a revised set of NNSA specific cyber security policies. However, successful implementation of these new policies will hinge on comprehensive oversight by each of the respective NNSA weapons laboratories local site office. Our most recent inspections at the NNSA weapons laboratories have identified inconsistencies where we noted excellent site office cyber security program oversight at Sandia, but less than effective oversight at the Los Alamos Site Office and Lawrence Livermore Site Office.

Unclassified Cyber Security

Now I would like to transition my testimony from classified cyber security to the unclassified environment. Unclassified computers and networks have become as much a part of our everyday lives as telephones and fax machines. Our national laboratories are no exception to this societal trend. As our reliance on these systems has increased, so has the type of information that we store on them, from personal information, such as social security numbers, to information that is unclassified, but sensitive enough that it could aid our enemies in damaging the national and/or economic security of the U.S. Examples might include unclassified controlled nuclear information and export controlled information.

In years past, the primary threats to our unclassified networks were directed at our perimeter defenses and, as a result, the Department directed significant effort toward strengthening its network perimeters. Firewalls and intrusion detection systems were implemented to repel and detect unauthorized access attempts into areas of the networks where sensitive information was

stored and web servers and other "public facing" systems were placed in special network segments, thus preventing them from becoming platforms from which to attack more sensitive information. Over the past several years our inspections have validated the success of this strategy in dealing with direct external attacks. However, as external network defenses have grown stronger, our adversaries have shifted strategies, and most attacks today are less direct.

In fact, almost all network penetrations now occur as a result of an authorized user activating a malicious software program, commonly known as a Trojan horse. These programs can be delivered either as attachments to email messages or via links to malicious websites. They may also be installed by merely inserting an innocent looking compact disk or thumb drive that contains a malicious program into a computer. The point is that the adversaries no longer have to penetrate our systems from the outside – they merely have to trick authorized users on the inside into running their programs. Once a user activates a malicious program, a communication channel is established to the adversary's system, essentially ignoring the otherwise effective firewall.

Recognizing that we needed a better way of evaluating DOE sites in this new threat environment, HSS supplemented its existing inspection program back in January 2005 with an unannounced network testing program, commonly referred to as red teaming. While our team is relatively small when compared to teams that could be used by our adversaries, it has a broad range of core competencies that are designed to model the current threat. Using the methods described above, our red team has been able to point out a number of areas in need of improvement, as well as identifying some sites that were very well protected. In addition to identifying strengths and

weaknesses in security controls, red teaming provides an opportunity to evaluate the Department's ability to detect and disseminate information about attacks and how it evaluates them once they are detected so as to fully address the attacks. Our most recent red team activity, which focused on a non-NNSA part of the Department, resulted in our ability to take full control of two site networks and one smaller site office network. As a result, our red team downloaded very large quantities (gigabytes) of data, some of which was sensitive, without being detected. This level of access could also have allowed us to change data or otherwise impact its integrity, or impact the availability of the networks and, by extension, the ability to execute site missions. In addition to the access we gained at these sites, by installing our own malicious programs on a number of their laptop computers, we were able to make connections into other networks after the laptops were legitimately connected to these networks through authorized accounts. This demonstrated our ability to migrate throughout the Department into sensitive networks.

Mr. Chairman, my point in discussing our red team to such an extent is to highlight the fact that, while the threat has evolved, time honored cyber security tenets are still relevant for evaluating the risks to our networks and determining appropriate countermeasures to mitigate those risks to an acceptable level. This was accomplished to some extent when, following an earlier red team that involved NNSA and DOE Headquarters, HSS worked with the DOE Chief Information Officer and Program Office representatives to develop a list of recommendations to combat today's network attack methods. Some of the technical countermeasures included controlling outbound network connections, blocking malicious email attachments, and using stronger password encryption processes. Programmatic recommendations included updating cyber

security policies, establishing a new governance model, and improving the processes for disseminating threat information and handling cyber security incidents.

While there has been some improvement in the unclassified cyber security arena, including better segmentation of computer networks and improved vulnerability scanning and patching processes, HSS continues to identify problems in fully implementing some fundamental security controls at DOE and NNSA sites. For example, while some sites, particularly within NNSA, have improved their processes for controlling outbound network connections, many other sites have not fully implemented mechanisms to prevent malicious software programs from sending sensitive unclassified information to sources outside their networks.

The Department also continues to struggle in the area of unclassified cyber security incident response, as demonstrated by our recent red team exercise, and judging by the inconsistency in implementing improved technical countermeasures, the new governance model has not matured to the point where it is fully effective. Efforts to improve the dissemination of current threat information to those who are responsible for making important risk management decisions have shown some improvement, but many sites do not have the infrastructure to receive and access classified threat information. DOE and NNSA unclassified cyber security programs also share many of the same problems in the areas of certification and accreditation, in that accreditation boundaries are not always clearly defined and certification tests do not always include all relevant system components.

Finally, I would like to go back to my earlier statement about the importance of implementing basic cyber security tenets, and in particular, risk management. The risk management process begins with the identification of threats and determining which assets are at risk from those threats. Only then can appropriate countermeasures be applied to mitigate the risks to a level deemed acceptable by competent authority. However, within the Department, we have not performed well in the area of risk management. In particular, the Department does not have a comprehensive understanding of the types and locations of sensitive information on our networks, including the sensitive "yellow" networks at our weapons laboratories. Some categories of sensitive information, such as unclassified nuclear information and naval nuclear propulsion information may warrant additional security controls beyond the minimum standards specified in Departmental and National policies. Additional controls could include encrypting some types of data during storage and transmission, or in extreme cases, removing it from the networks.

Mr. Chairman, we know that the threat will continue to evolve, and we know that our adversaries will continue to obtain footholds within our unclassified networks. We also know that we have not done all we can to prevent them from gaining those footholds and from exporting sensitive data outside the control of the Department. Our networks contain various categories of sensitive information and, while sites have made efforts to protect it through network segmentation, our red teams have shown that our adversaries could still get to the information and still export it from the Department's networks. While the DOE Chief Information Officer and Under Secretaries have made notable progress in recent years with respect to developing new policy and a governance model through which to implement the new policies, our inspections and red

teams have continued to demonstrate that some fundamental cyber security requirements are not consistently implemented throughout the Department. Essentially, the governance model enables Under Secretaries to determine how they will implement Departmental requirements through their Program Cyber Security Plans. While this model has merit in a large, diverse organization such as DOE, its effectiveness hinges on the extent to which the DOE Office of the Chief Information Officer ensures that the Under Secretarial Program Cyber Security Plans comply with the overarching DOE policies. Our inspection activities continue to identify areas in which these DOE policies are not required.

Therefore, to protect sensitive information more effectively, we will need to enhance certain aspects of Departmental policy, such as requiring encryption of sensitive information stored on all computers. Current policy requires encryption (e.g., Entrust) for sensitive information such as unclassified nuclear information and personally identifiable information, but only when it is stored on portable devices. The Department should also implement a more robust Program Cyber Security Plan compliance review process by the DOE Chief Information Officer to ensure that the plans meet expectations. DOE Under Secretaries should also revisit some of the risk decisions that have been made, with particular emphasis on the evolving threat environment.

While there are a number of possible improvements that would result in significantly raising the bar for potential intruders, I do not want to understate the work that has already taken place and some sites, especially within NNSA, have addressed most of the recommendations to some extent. However, as you know, the Department continues to identify successful penetrations of our networks. With respect to improving our ability to keep intruders from gaining a foothold in

our networks, we should continue to educate our users regarding the threats involved with opening attachments and running programs from untrusted sources. But while user education will reduce the number of malicious programs executed on our networked systems, we must also assume that some users will still make mistakes and execute these programs. Therefore, we should implement authenticated gateways for all outbound Internet access. Essentially, this means that users would have to log in to the gateways to reach the Internet. This would greatly reduce the ability for automated programs, such as Trojans, from establishing pathways to external systems. We should also continue to move toward multifactor authentication for all access to computers, whereby users would have to use at least two types of authentication, such as a password and a periodically changing code from a token. Finally, we should continue to improve vulnerability scanning and automated security patching processes, which will result in the presence of fewer exploitable vulnerabilities on our networks.

While the aforementioned security enhancements will significantly reduce the risks to our networks, we must also assume the worst case scenario, wherein some attackers will succeed in gaining access to our networks. In these cases, we need to make it more difficult for intruders who do manage to establish footholds to migrate to other areas of the site networks. Some of the solutions involve nothing more complicated than changing configuration settings on computers, while others require improving network infrastructures. We should discontinue the practice of using a single administrator password to manage multiple computers. Our red teams routinely demonstrate that once we gain access to an administrator password, we are able to scan the network for all other systems that use the same password and gain access to many other systems with no additional effort. We should also discontinue the practice of allowing general users to

have administrator level privileges on their computers. If the users do not have administrator privileges, attackers who gain access to the systems do not have sufficient privileges to install malicious programs such as keystroke loggers. From a network infrastructure perspective, we need to increase intrusion detection capabilities within our networks. A mixture of network-based and host-based mechanisms would significantly increase the risk of exposure for attackers who are trying to migrate through the networks. Also, we should aggregate all security logs to a central system to more efficiently analyze suspicious activities and to correlate events and identify related activities across the network.

Finally, we need to do a better job of keeping attackers who manage to gain access to sensitive information on our systems from sending that data outside our network perimeters. We should also evaluate all network trust relationships to verify their necessity and to restrict those that are necessary to the minimum connectivity required. We should block outbound access through all network ports, except those that are specifically needed and we should use proxy servers to better protect those services that are specifically authorized. Proxy servers act on behalf of computer users by exchanging data with remote servers without making direct connections. Because proxy servers are specifically configured for each network, automated malicious programs are much less likely to successfully establish a communications channel to the attackers' networks.

Mr. Chairman, members of the subcommittee, we are capable of doing these things right now. In fact, there are commercial solutions available to perform most of these tasks. And where a gap in available products exists, we should take the necessary action to identify and deploy better tools to monitor and control network interfaces.

Conclusion

Mr. Chairman and members of the subcommittee, I believe all here in this room share the goal of ensuring that our national security assets are rigorously protected and also share the concern when protection effectiveness falls below our standards. The Department's commitment to protecting the assets in our custody is unwavering. Despite the difficulties associated with the age and configuration of some facilities, results of our evaluations indicate an overall trend of improving security as the sites – including the NNSA weapons laboratories – continue to implement Departmental security initiatives, consolidate special nuclear materials, and correct problems of the past. However, there are still chinks in the armor. Some deficiencies in various protection system layers have not yet been fully corrected, and periodically we discover new deficiencies. While it may be nearly impossible to provide one hundred percent assurance of protection system effectiveness, particularly for information assets that are accessed by many employees daily in the line of duty, we believe the weapons laboratories can and must improve their performance in this area.

Line managers responsible for the weapons laboratories need to sustain efforts to address known deficiencies, sustain support for ongoing and future initiatives aimed at countering evolving threats, and strive to implement fully effective protection systems. As long as we have assets to protect and adversaries who threaten them, such efforts will be perpetual. There are and always will be deficiencies to correct and improvements to be made. However, I can say with confidence that the laboratories have implemented protection systems that provide reasonable

assurance that special nuclear materials are protected from unacceptable levels of risk. I can say with equal confidence that while we have identified no catastrophic vulnerabilities in their information protection programs, the laboratories have additional work to do to ensure that their efforts to protect the millions of items of classified information that they possess in physical and electronic form fully meet the Department's expectations. Finally, in the area of unclassified cyber security, I cannot stress strongly enough my belief that we need to get back to the basics of risk management to identify which information needs special protection, to determine appropriate protection measures to apply to that information, and then we need to ensure that the protection measures are actually implemented. In conjunction with these efforts, we must deploy better tools to monitor and control our network boundaries.

This concludes my remarks. Thank you for the opportunity to express my views on security at the national weapons laboratories.