

## **Lawrence Livermore National Laboratory's Security Posture**

Hearing of the House Committee on Energy and Commerce  
Subcommittee on Oversight and Investigations

September 25, 2008

Dr. George H. Miller, Director  
Lawrence Livermore National Laboratory

### **Opening Remarks**

Mr. Chairman and Members of the Committee, thank you for the opportunity to provide my perspective on the security challenges facing the Lawrence Livermore National Laboratory (LLNL) and the other NNSA laboratories. I am George Miller, Director of LLNL and President of Lawrence Livermore National Security (LLNS), which has been managing the Laboratory for almost one year. I started at LLNL in 1972 as a research physicist in the nuclear weapons program. In my career I have had responsibilities at every level of management at LLNL. As a national security laboratory, we are very familiar with the threats to our nation and take very seriously the special responsibilities entrusted to us to protect special nuclear materials (SNM) and some of the nation's most sensitive secrets. Particularly in the cyber area, threats are rapidly evolving and continue to grow more sophisticated. Vigilance and continuous improvement are required.

The Laboratory's approach to both physical and cyber security employs a multi-layered, defense-in-depth strategy with opportunities for regular feedback, assessment, and improvement. This process draws on both internal and external assessments and I will report on the aggressive actions LLNL is taking to continue to strengthen both physical and cyber security. Recently, DOE's Office of Health, Safety, and Security (HSS) conducted an inspection of LLNL

Safeguards and Security and Cyber Security, and found areas of effective performance, areas needing improvement, and some areas of significant weakness. We took immediate action to respond to these findings and have made significant progress. Recently the NNSA Office of the Chief of Defense Nuclear Security stated that improvements made in LLNL Protective Force response capabilities since the HSS inspection “have resulted in a robust protection strategy.” In the area of cyber security, the HSS report concluded that the Laboratory faces challenges but “...has the teams, technologies, and methods needed for success to effectively address cyber security program needs.” We are drawing on those capabilities to expeditiously make necessary improvements.

### **Laboratory Security and the Recent HSS Inspection**

I can assure you that LLNL is committed to the safe and secure fulfillment of its mission responsibilities. The Laboratory takes an integrated approach to safety and security with a commitment to continuous improvement. Safety and security are the most important considerations in day-to-day operations. A fundamental value of the Laboratory is for all employees to take personal and collective responsibility for providing for a safe and secure work environment.

An extensive security infrastructure is in place at the Laboratory, and continual improvements are made to address new threats and arising concerns. LLNL uses a defense-in-depth approach to physical security that includes fences, buildings, doors, repositories, and vaults with various levels of access control in addition to aggressive armed defense and response capabilities protecting the Superblock Facility, the special area where work with SNM is conducted.

Cyber security is a growing and rapidly evolving defense challenge for all government entities, including the NNSA laboratories. Cyber attacks are a serious national security threat that require interagency attention, cooperation, and investment to improve protection. Recognizing the public trust placed in the Laboratory to protect some of the nation's most sensitive secrets, LLNL takes its cyber security responsibilities very seriously. The Laboratory employs an integrated management approach to protect its cyber resources in an ever changing threat environment. LLNL leverages expertise in security management, counterintelligence, and information technology to identify and quickly respond to emerging threats and proactively develop and deploy protective measures. Most importantly, classified information at LLNL is secure. It is confined to networks that are isolated and segmented to ensure need-to-know access and well protected by technical processes that provide both system and information security.

Unclassified computing at LLNL is separated into individually protected, NNSA accredited, network segments that include a Green network, a Yellow network, and a new Blue network. Through the use of firewalls, authorization codes, and other means of security, this segmentation allows for greater control and increasing levels of hardware and data protection depending on the types of data and applications that are on each of the networks. The Yellow network, which is subsequently discussed in more detail, is the main unclassified network for desktop computers, applications and databases, unclassified programmatic activities, internal communications, and business services. Employees receive and send email, fill out their time card, do their on-line training, work on technical data and information, and access benefits and other employment information on this network. It does contain sensitive unclassified information such as business

proprietary and personnel information that is segregated within the Yellow network with additional access controls. The Yellow network is restricted to Laboratory employees and collaborators. Connected to the Internet, this network is protected by a robust firewall and network segments that must be diligently maintained in the face of ever more sophisticated threats.

The Blue network has recently been piloted and is now approved for expansion. Its purpose is to provide controlled access to assets necessary for our foreign national employees and collaborators to do their work, but at the same time restrict their access to resources on the Yellow network. The Green network is lightly firewalled and provides public access to general LLNL information including job postings.

The Laboratory utilizes a variety of tools to continually assess and test both physical and cyber security. These include Government Accountability Office (GAO) audits, on-site inspections by DOE's HSS, local NNSA site office surveys, self-assessments, risk assessments, vulnerability scanning, and system testing conducted by the LLNL cyber security program. These assessments provide valuable input and are an integral component of LLNL's continuous improvement process to sustain the Laboratory's security in an evolving threat environment.

In early March 2008, DOE HSS initiated an inspection of LLNL Safeguards and Security and Cyber Security. Over a six-week period, 86 auditors participated in a comprehensive evaluation of eight security elements. The inspection was conducted with a high level of professionalism. For example, the composite adversary team that conducted the force-on-force exercise was very

experienced and innovative in their approach, and they conducted the force-on-force exercise in a manner to test LLNL's Superblock Facility security posture to specific criteria. We value the approach taken by HSS in all facets of its inspection and the receipt of in-depth feedback to improve our security posture.

In summary, the HHS inspection found LLNL to have effective performance in Classification and Information Control, Personnel Security, and Material Control and Accountability. HSS found that the Laboratory needed improvement in Physical Security Systems, Protection Program Management, and certain aspects of Cyber Security not related to technical controls. HSS found significant weakness in LLNL's Protective Force and its Classified Matter Protection and Control.

The Laboratory took immediate steps to address weaknesses identified in the HSS inspection. In addition, LLNL developed a comprehensive set of corrective action plans. HSS reviewed the Laboratory's draft corrective action plans and HSS comments have been incorporated into the plans. These draft plans contain 254 milestones to correct and sustain LLNL's progress toward ensuring a long-term, strengthened security posture. Aggressive efforts to sustain NNSA site security compliance requirements have resulted in the completion of one-third of the milestones to date.

The results of the HSS force-on-force exercise were disappointing to me and my team. The Laboratory's Protective Force had performed well in the prior HSS force-on-force exercise only 16 months earlier (December 2006), and I was determined to identify the root cause leading to

the decline in the Laboratory's Protective Force readiness. I immediately ordered a thorough review of our actions and decision making to identify and correct the root cause. In short, the analysis revealed that restrictions on and postponements of robust exercises had a detrimental effect on Protective Force readiness as well as our ability to conduct the full-scale exercises that are necessary to appropriately practice team tactics and fully assess performance. The lack of a robust exercise environment inhibited the Laboratory's ability to obtain the necessary feedback to assess our performance.

Safety considerations and attrition in LLNL's Protective Force were some of the most influential factors that placed limitations on exercises. For example, the Laboratory's initiative in 2006 to improve ladder safety practices resulted in the suspension of force-on-force exercises on the roofs in the Superblock. In addition, NNSA's prohibition on the use of smoke due to health concerns prevented us from utilizing this tool in our training. Other concerns regarding Superblock employee health and safety further restricted the ability of our Protective Force officers to engage in realistic exercises inside Superblock facilities.

Another contributing factor was attrition in the Laboratory's Protective Force, which has averaged about 10 percent per annum, FY 2006 through FY 2008. Force-on-force exercises in the Superblock are labor intensive, requiring sufficient Protective Force personnel to participate in defensive and offensive teams, help conduct the exercise, and to provide a stand-alone force to protect the area during the exercise. With high attrition and a two-year training regiment for new officers, shortfalls in staffing required careful workload balancing and significant overtime to provide defense, train, and exercise.

The limitations emanating from these considerations resulted in Protective Force exercises that were insufficient in scope and degree of realism to identify weaknesses in equipment performance and team tactics.

We took actions to address this root cause. First, we devoted special attention to expeditiously resolve safety concerns by, for example, marking and providing guide structures on roofs for safe access and providing ventilation within hallways so that blank ammunition can be used. Once we resolved these concerns, we resumed robust exercises in the Superblock, and will conduct robust force-on-force exercises on a quarterly basis. Second, we reinvigorated our physical security self-assessment program and assigned a seasoned security professional to a newly created position as the Security Organization Program Performance Assurance Manager. Finally, we took away valuable lessons from each of the factors that contributed to decisions that had self-limited exercises and assessments.

We have applied the lessons learned from all facets of the HSS inspection. Working closely with NNSA and utilizing expertise accessible through reachback to LLNS parent organizations, LLNL has significantly strengthened its security posture over the last several months. Highlights are discussed below in the areas of Protective Force, Classified Matter Protection and Control, and Cyber Security. In addition, the Laboratory has implemented management changes to clarify roles and responsibilities through an integrated chain of command that incorporates expertise in SNM research, safety, and security. Vulnerability assessments are being updated to include the recent protective force, physical security, and cyber security enhancements.

## **Protective Force Improvements**

LLNL has implemented improvements to its manpower deployment and training, to its defensive equipment, to its command and control systems, and continues to implement improvements to its hardened fighting positions in the Superblock. These improvements were guided in part by the lessons learned during a period of intensive activity in May and June 2008 when over 25 scrimmages, limited-scope performance tests, and 12 force-on-force exercises against a variety of adversary teams were conducted in the Superblock Facility exercising all LLNL Protective Force shifts. The Laboratory's integrated plan ensures a high-quality training environment with the appropriate equipment resources to continually challenge and test the responsiveness of its Protective Force. LLNL has implemented Protective Force improvements in four areas: Personnel, Equipment, Team Tactics, and Training Environment.

*Personnel.* The HSS Inspection found that LLNL's Protective Force security officers were individually well trained and capable as demonstrated by their high test scores. This is due in part to LLNL adopting the newly proposed Tactical Response Force (TRF) Standards as part of its training. LLNL is currently the only site in the complex to qualify all of its Level 2 and 3 Protective Force officers in this weapons and physical fitness proficiency standard.

Lessons learned from HSS force-on-force exercise, and the subsequent force-on-force exercises, resulted in the addition of Protective Force officers in the Superblock Facility on each shift, and the addition of a Sergeant to each shift to engage exclusively in Command and Control. Both of

these actions have been completed and are incorporated into the Security Incident Response Plan (SIRP).

*Equipment.* LLNL utilizes Dillon gatling guns, integrated into Mobile Weapon Platforms (MWP), as part of the security posture for the Superblock Facility. Since the HSS inspection, LLNL has developed a robust security incident response plan that utilizes a MWP deployment strategy that does not rely upon all vehicles being deployed at all times. This plan allows LLNL to deploy some or all of the vehicles and maintains a high level of protection by augmenting and re-deploying forces within the Superblock in towers, bullet-resistant enclosures, hardened-fighting positions, or as ground-based strike teams. Consequently, this plan protects the SNM and provides for cycling vehicles out of the Superblock Facility for necessary vehicle service, vehicles to conduct training, and the ability to upgrade vehicle systems without degrading LLNL's protection effectiveness. In addition, it forces an adversary to develop a plan and commit resources to address multiple protection strategies—a much bigger task for an adversary than would be required to deal with a static protection configuration.

We have upgraded the defensive equipment used by our officers to protect the Superblock including improvements to the MWP that mitigate maintenance and reliability issues. In addition, the operability of the MWPs is verified each shift.

*Team Tactics.* Daily and nightly training began and has continued since April to ensure effective implementation of the SIRP and verify compliance of the Protective Force officers with it. These training exercises and Limited Scope Performance Tests involve individual, small unit, and full

team movement and tactics. Refinements to command and control protocols have been developed based on these exercises, as well as actions to address security officer vulnerabilities identified during the exercises.

*Training Environment.* In order to facilitate more realistic training, LLNL engages in force-on-force activities in the Superblock Facility and indoors with realistic Multiple Integrated Laser Engagement System (MILES) gear on a routine basis. During the first week of August 2008, a fully integrated force-on-force exercise was conducted by an adversary force from Idaho National Laboratory. This force-on-force exercise was attended by representatives of the Office of the Chief of Defense Nuclear Security, NNSA Field Security professionals, and observers from DOE HSS. The force-on-force exercises were particularly challenging, designed to test the changes to our SIRP and the additional training of our security force. LLNL's security incident response was very successful. The Office of the Chief of Defense Nuclear Security asserts, "The results of the exercises demonstrate that activities completed as part of the site recovery plans, along with the planned configuration, have resulted in a robust protection strategy."

### **Improvements in Physical Security Systems and Classified Material Protection & Control**

LLNL's security construct is based on a series of defensive layers—a graded approach that provides increasing barriers that correspond to the increasing security value of critical Laboratory assets. Classified information resides in "limited" areas and is stored in repositories and/or vault-type rooms (VTRs). Some of LLNL's VTRs were found to be deficient in sensor protection by the HSS inspection, and the necessary additional sensors were immediately installed.

In addition to enhancing the VTRs, LLNL formalized roles and responsibilities, and improved VTR configuration management. The Laboratory is consolidating databases that document the location of classified repositories into a master database and has established a policy and verification procedures for configuration control of classified repositories and VTRs. In addition, procedures for logging and inventory of failed classified computer hard drives now address concerns raised by the HSS inspection. LLNL has upgraded the lighting and video coverage in the Superblock.

### **Cyber Security Improvements**

As an integral component of LLNL's security organization, the Laboratory's cyber security program proactively develops and deploys effective defensive systems and quickly responds to emerging threats to ensure appropriate protection. The cyber security program takes an integrated approach, strongly engaging counterintelligence experts and information technology professionals. The Laboratory has established centralized policies and procedures for managing cyber security, and it has in place many effective technical processes and tools for providing protection. These include perimeter and internal firewalls, vulnerability scanning, and intrusion detection systems. In addition, the Laboratory has developed and utilizes an effective system for user identification, authentication, and access control to enforce security standards and ensure appropriate configuration management of software and hardware systems.

The HSS inspection rated LLNL's cyber security technical controls "effective" and found that the cyber security program "has taken an aggressive stance to ensure that when issues are

recognized, corrective action plans and plans of action and milestones are developed.” In response to deficiencies identified in the HSS report, LLNL is strengthening its cyber security controls for planning, acquisition, certification, and accreditation of systems to reduce overall risk. The Laboratory is updating its cyber security plans to reflect the most up-to-date directives and include more detailed operational protocols in order to better test, certify, and accredit systems.

Classified information at LLNL resides on separate networks for Secret/Restricted Data and Secret/National Security Information, a practice HSS found “commendable.” Their report concludes that, “Strong identification and authentication controls for access to applications and effective segmentation to ensure need-to-know boundaries, as well as effective vulnerability scanning and patching, are key factors in the classified environment being almost totally devoid of vulnerabilities.”

As mentioned earlier, the Yellow network at the Laboratory is the main unclassified network for desktop computers, applications, and databases. This network contains access-controlled sensitive unclassified information that is required by most Laboratory employees and collaborators to conduct their mission responsibilities. It is the backbone for unclassified programmatic activities, internal communications, and all business services. Laboratory research, business functions, and operations require external communications; hence, the Yellow network is connected to the Internet and protected by a firewall and network segments.

Vigilance is required to protect Yellow network systems and data. LLNL first completed a comprehensive sitewide unclassified risk assessment in 2005. Updated annually and as new risks are identified, the assessment includes an analysis of systemic conditions and threats, probabilities of occurrence, and impact. Consideration of the risks guides strategies for vulnerability scanning and patching as well as the implementation of additional measures to limit inward and outward flows through the firewall. The Laboratory is working to fully implement effective risk management processes to identify risks at the system-specific level.

One notable step LLNL is taking to minimize risks is the development of a Blue network. To be used by foreign nationals whose collaboration is necessary for LLNL to meet mission responsibilities, the network was established to provide even greater assurance that access restrictions to LLNL information systems are enforced based on need-to-know. The Blue network segment is separated from the Yellow network through technical controls. Users have access only to approved resources on the Yellow network and that access is only permitted with controls enforced by firewall policy. This prevents foreign nationals from having the ability to “knock on doors” and gain access to Yellow network resources on an uncontrolled basis. They are not able to search the Yellow network or monitor activities on it. The Blue network is being piloted in one of the Laboratory’s directorates and is planned for site-wide implementation in Fiscal Year 2009.

### **Closing Remarks**

The Laboratory requires annual training for every LLNL employee to ensure that each understands the importance of protecting the classified information and materials at the

Laboratory and their individual and collective security responsibilities. Security is an obligation that we take extremely seriously. The adversarial threats we face are growing more sophisticated and defense requires vigilance. When deficiencies are uncovered or an emerging threat is identified, we act as promptly and effectively as we can to fix the specifically identified issue as well as address the root causes. That is why the Office of the Chief of Defense Nuclear Security was able to assert that LLNL's concerted efforts "...have resulted in a robust protection strategy" after shortcomings were uncovered by HSS only several months earlier. I have confidence in LLNL's Protective Force and the effectiveness of the Security Incident Response Plan.

Cyber security is a challenge facing all government entities, including LLNL. I agree with the HSS report that concluded "the laboratory has the teams, technologies, and methods needed for success to effectively address cyber security program needs." LLNL welcomes the opportunity to share some of the lessons we have learned—and to learn from others—through broader, more concerted, and effectively-integrated DOE and interagency efforts to cope with this very serious national security threat.

## **Lawrence Livermore National Laboratory's Security Posture—Summary (Attachment)**

Lawrence Livermore National Laboratory (LLNL) is committed to the safe and secure fulfillment of its mission responsibilities. A fundamental LLNL value is that all employees must take personal and collective responsibility for providing for a safe and secure work environment. An extensive security structure is in place at LLNL, and we are taking aggressive actions to address arising security threats and concerns. Particularly, in the cyber area, threats are rapidly evolving, continuing to grow more sophisticated and vigilance is required.

The Laboratory benefits from both internal and external assessments to identify weakness and areas for improvement. Recently, DOE's Office of Health, Safety, and Security (HSS) held an inspection of LLNL Safeguards and Security and Cyber Security that provided valuable feedback. We took immediate steps to address the identified weaknesses. We conducted a thorough review to identify the root cause of the disappointing results of the force-on-force exercise and took corrective actions. Restrictions on and postponements of robust exercises had a detrimental effect on Protective Force readiness and inhibited the Laboratory's ability to obtain essential feedback on our performance. We resumed the conduct of realistic force-on-force exercises in the Superblock, and we will conduct future comprehensive force-on-force exercises on a quarterly basis. We have also upgraded the defensive equipment used in the Superblock. Following a fully integrated force-on-force exercise in August 2008, the NNSA Office of the Chief of Defense Nuclear Security, improvements made in LLNL Protective Force response capabilities "have resulted in a robust protection strategy."

In the area of cyber security, the HSS report concluded that "the classified environment [at LLNL is] almost totally void of vulnerabilities." LLNL's (unclassified) Yellow network faces challenges, but it is well protected and the HSS report states that LLNL "has the teams, technologies, and methods needed for success to effectively address cyber security program needs." We are drawing on those capabilities to expeditiously make improvements, including the development of a new Blue network for use by foreign national employees and collaborators.

## Lawrence Livermore National Laboratory



### **DR. GEORGE MILLER**

Director

Lawrence Livermore National Laboratory

B.S. physics, College of William and Mary (1967)

M.S. physics, College of William and Mary (1979)

Ph.D. physics, College of Williams and Mary (1972)

Dr. George Miller is the tenth Director of Lawrence Livermore National Laboratory, a position he assumed in March 2006, after a long and distinguished career in national security work at the Laboratory. While serving as Director, Dr. Miller is responsible for the management of the Laboratory and led the institution through its transition to a new management contractor, Lawrence Livermore National Security (LLNS), LLC, in October, 2007. Dr. Miller also serves as the President of LLNS.

Throughout his tenure, Dr. Miller has tackled a variety of management and scientific challenges in the interest of national security. For example, under Dr. Miller's leadership as Associate Director for the National Ignition Facility, a new management team was assembled in 1999 with a new project execution plan that put it on track for completion in 2009. Through Dr. Miller's stewardship, this \$3.5 billion laser continues to meet all of its milestones on time and cost.

Prior to his position at NIF, Dr. Miller provided the leadership to integrate LLNL's national security programs into a cohesive effort to meet U.S. national security objectives of maintaining the U.S. nuclear deterrent without nuclear testing, advance national nonproliferation and arms control goals through the development and application of effective scientific and technical solutions, and support DOD programs.

From 1985 until 1996, Dr. Miller led the Laboratory's nuclear weapons program as a major participant in the development of the Stockpile Stewardship and Management Plan to ensure the safety, security and performance of the nation's nuclear deterrent in the absence of testing. Dr. Miller applied his expertise as a weapons design physicist to assist in the development of the scientific capabilities necessary to maintain the nuclear deterrent without nuclear testing. He developed his scientific management skills as the project leader for the B77 nuclear weapon development and the W84 ground launched cruise missile.

Dr. Miller has represented the Laboratory's national security programs to a wide variety of decision makers in the federal government, including members of the Executive Branch, Departments of Energy and Defense, and the U.S. Congress. In 1989, Dr. Miller provided scientific counsel to Secretary of Energy Admiral James D. Watkins while on a temporary assignment to the Department of Energy as Special Scientific Advisor on Weapons Activities. He provides advice to the Commander of the United States Strategic Command through his membership on the USSTRATCOM Strategic Advisory Group and as Chairman of its Science and Technology Panel.

Dr. Miller holds memberships in the American Physical Society and Sigma Pi Sigma - National Physics Honor Society. He has received awards and honors from the National Science Foundation Graduate Fellowship, Gulf-General Atomics Fellowship, and Sigma Pi Sigma.