Testimony of Dr. Michael R. Anastasio
Director, Los Alamos National Laboratory

Hearing on "A Review of Continuing Security Concerns at DOE's National Labs"

Before the Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
U.S. House of Representatives

September 25, 2008

Executive Summary

I am Dr. Michael Anastasio, director of Los Alamos National Laboratory. From my first appearance before the Subcommittee in January 2007, I understood the message from the Members — continued security issues were not going to be tolerated. I am pleased to report that Los Alamos National Laboratory is now demonstrating a track record of security successes, in both physical and cyber security.

The concrete actions we have taken to reduce our risks, clarify security roles and responsibilities, and develop solutions to continuously improve our overall security posture are working.

I am particularly proud that the improvements made at the Laboratory link directly back to the actions and attitude of our employees. The changes by the employees have been coupled with an aggressive security improvement campaign, where the Laboratory has:

- Reduced the number of Vault Type Rooms (VTRs) from 142 to 108;
- Reduced our Accountable Classified Removable Electronic Media (ACREM) from 12,000 items to 3,900 items in just over two years;
- Opened the first Super VTR, and are planning the deployment of four more;
- Converted 94 percent of our targeted classified workstations to diskless operation;
- Destroyed more than 40,000 classified nuclear weapons parts;
- Destroyed more than 3 million non-accountable classified documents;
- Begun development of a segregated unclassified cyber network for our foreign national employees and of two new cyber protection technologies to better protect our unclassified networks.

I am also encouraged that in three recent external assessments—both the Government Accountability Office and the DOE's Office of Health, Safety, and Security—validated the significant positive progress we are making. However, these reports also clearly demonstrate we have need for further improvement, especially in the area of cyber.

Continuous security improvement is essential and nowhere is this more evident than in the area of cyber security. The cyber threat is my greatest concern, as I expressed in my last appearance before you—an ever-increasing, evolving threat from persistent, technologically adept adversaries.

Of course, protection of our classified resources is our highest priority, but securing our unclassified Yellow network is also essential—it is the backbone of our operations and communications activities. Developing solutions that both manage the risk and allow user functionality for daily operations is crucial.

However, it is clear that this is a threat the whole nation is facing and something that requires a coordinated national response. The national laboratories' unique cyber capabilities, building on our ongoing integration efforts, can be a valuable resource in that response.

Introduction

Chairman Stupak, Ranking Member Shimkus, and Members of the Subcommittee, thank you for the opportunity to appear this morning to discuss the physical security and cyber security challenges that the national laboratories face. It has been more than a year since I last appeared before you, and I am pleased to report that Los Alamos National Laboratory has made a great deal of progress to meet these increasing and ever-evolving security challenges.

I am Dr. Michael Anastasio. I have served as the director of Los Alamos National Laboratory since June 2006. I am also the president of Los Alamos National Security, LLC, (known as LANS) the company whose sole purpose is management and operation of Los Alamos National Laboratory. As president of LANS, I report to the LANS Board of Governors, which includes representatives from LANS's four member organizations: Bechtel National, the University of California, Babcock & Wilcox, and URS. My Board plays a very strong oversight role and holds both the Laboratory and me personally accountable for our progress. One of the oversight subcommittees of the Board is focused exclusively on safeguards and security, and the members of that subcommittee have helped us to make progress in this area.

Los Alamos carries out very important responsibilities for the nation, most notably our primary mission of maintaining the safety and reliability of the nation's nuclear weapons deterrent. Central to that and other missions is the ability to protect and handle classified information and assets. All three laboratories are working vigilantly to address known risks

and to anticipate emerging threats, and I want the Committee to know that I personally take the issue of security very seriously.

Mr. Chairman, during my last appearance before the Subcommittee, I specifically outlined in my testimony three areas encompassing physical and cyber security where we would focus our continuous improvement efforts. Those three areas included:

- Reducing and consolidating our classified holdings;
- Changing employee security behavior by developing consistent and clear security policies; and
- Sustaining our corrective actions with continuous improvement.

Today, the Laboratory continues to make significant progress in each of the areas I outlined in my testimony. More specifically the Laboratory has:

- Reduced the number of Vault Type Rooms (VTRs) on site from 142 to 108;
- Created and implemented controls for all classified computer ports;
- Reduced our Accountable Classified Removable Electronic Media (ACREM) from 12,000 to 3,900 in just over two years;
- Opened the first Super VTR, and is planning the deployment of an additional four;
- Converted 94 percent of our targeted classified workstations to diskless operation;
- Deployed (and continue to refine) its Integrated Safeguards and Security Management System (ISSM);
- Destroyed more than 40,000 classified nuclear weapons parts;

- Developed and is implementing a program to secure all of its classified nuclear weapons parts in standard storage by July 2009;
- Started and continue development of a segregated unclassified cyber network for our foreign national employees;
- Began to develop and adopt new cyber protection technologies such as “glove box computing” and “threat resilient networks.”

The Laboratory has made significant, demonstrable progress, but I know that we are not yet finished. As any security professional will tell you, security is a continual battle. This is especially true in the area of cyber security where we are facing mounting challenges from external threats to our unclassified systems. The Government Accountability Office (GAO) specifically highlighted the Laboratory’s unclassified cyber challenges, which I believe apply across the entire federal government.

As I will discuss, many of the reports and audits of Los Alamos security call out areas where we need to improve or where we need to make more progress. I agree with most of these assessments. By applying project management discipline, we are addressing these issues as quickly and effectively as possible in a systematic manner to achieve the best program with the available resources. I will give a brief description of each of the reports and audits, and I will provide greater detail on our specific responses to the reports in the progress update section of the testimony.

Recent reports and audits

The Laboratory receives a great deal of internal and external oversight. We welcome this attention, both from this Committee, as well as from the other bodies that have jurisdiction over our efforts. During the past year, our security operations have been audited more than 10 times. In my testimony, I would like to focus on three of the most recent audits—two conducted by the GAO and one by the DOE's Office of Health, Safety, and Security (HSS). They include:

- The GAO Report 08-694 on "Long Term Strategies Needed to Improve Security and Management Oversight";
- The GAO report 08-961SU on "Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network"; and
- The HSS security audit led by Glenn Podonsky that was completed just one week prior to today's hearing.

Let me first address the GAO Report 08-694 titled "*Long Term Strategies Needed to Improve Security and Management Oversight*," May 2008.

We appreciated GAO's detailed analysis of both the progress made at the Laboratory and the three specific areas where the auditors had concerns. I was encouraged that the GAO found that "LANL has over two dozen initiatives underway that are principally aimed at reducing, consolidating, and better protecting classified resources, as well as reducing the physical footprint of the laboratory by closing unneeded facilities."

The GAO did raise concerns related to “non-standard” storage of classified parts, weaknesses in our corrective action processes, and whether the improvements that we have made will prove sustainable. Later in my testimony, I will focus on each of these concerns, and the plans that we have in place to address them.

The GAO issued a second report (08-961SU) focused more on cyber issues titled “*Information Security: Actions Needed to Better Protect Los Alamos National Laboratory’s Unclassified Computer Network.*”

This recent report from the GAO provides a comprehensive analysis on steps needed to ensure that the Laboratory’s unclassified network is protected from attack. Some of the recommendations have been completed already, while others are being implemented or evaluated against alternative approaches determined during the accreditation risk assessments. These recommendations have been incorporated into our information security architecture and coordinated corrective action plans are being developed to build sustainable solutions for evolving threats.

The report notes that “LANL has implemented measures to enhance its information security, but weaknesses remain . . . on its unclassified network.” The GAO recommendations focus most directly on the issue of risk assessment and the ability of foreign nationals to access the Laboratory’s unclassified network, calling for the Laboratory to “ensure that the risk assessment for the unclassified network evaluates all known vulnerabilities and is revised periodically” and to “strengthen policies . . . further reducing, as appropriate, foreign

nationals'—particularly those from countries that DOE has identified as sensitive—access to the unclassified network."

The Laboratory has developed a formal cyber security risk assessment process. Further, the Laboratory is now developing a segregated unclassified computer network for utilization by our foreign national employees. This network will allow for greater control over what types and how information can be accessed while still allowing for important scientific research to be accomplished.

I generally agree with the findings in both GAO reports, but I want to note that LANL is demonstrating significant progress in dealing with our classified parts, understanding the risks to our computer networks and completing formal risk assessments for all classified and unclassified computing systems, and developing and implementing corrective actions that are not only sustained but continuously improved.

Finally, I will comment on the HSS audit titled "*August- September 2008: Results of the Los Alamos National Laboratory and Los Alamos Site Office Safeguards and Security Inspection*."

The Laboratory has been working closely with Health Safety and Security Director Glenn Podonsky and his team of professionals over the past two months on this most recent HSS audit. I personally—and the Laboratory as an organization—took this audit very seriously, and we viewed it as an opportunity to highlight for HSS the considerable progress that we

have made. We also view such audits as an opportunity to see where we need to apply additional resources.

I was pleased to see that the draft DOE inspection report recognizes the Laboratory for making significant progress in many security arenas. I was particularly gratified that the report stated that, “LANL has demonstrated significant progress and success in efforts to address longstanding deficiencies in its safeguards and security program. Notable performance improvements are evident in most major protection program elements, and significant corrective actions are underway to address remaining areas requiring improvement.”

Specifically, the draft report highlights Security Program Management, Protective Force Operations, Security Systems, Personnel Security and Classification as performing “effective performance,” HSS’s highest rating.

The two remaining areas, Material Control and Accountability and Classified Matter Protection and Control were rated as “needs improvement,” and our security team was already taking action to address the findings raised by the audit team. My expectation is that we will achieve effective performance in these two areas by next summer.

I do want to draw attention to the fact that in each of the previously mentioned reports and audits the organizations examining our operations call out the fact that they are noticing improvements in our security posture. A significant impetus for all these improvements is

our employees and the efforts they are making to oversee and execute their security responsibilities. This is one area with which I am extraordinarily pleased.

Los Alamos National Laboratory is making progress on the security front

Los Alamos National Laboratory has made significant changes and improvements in security since LANS took over in June 2006. The Board of Governors of LANS, LLC, my senior management team, and I have embraced the challenge of managing security risks at Los Alamos National Laboratory. While the Laboratory has not achieved all of its security-related goals, we have made very significant progress. External independent auditors, most notably the GAO, have taken note of our improvement efforts and successes to date. Let me detail some examples of the improvements that we have made. This list is by no means exhaustive, but it does suggest the magnitude of effort that we are making.

Physical security improvements at LANL

First, it's important to understand the general approach that we take to maintain and continuously improve physical security at the Laboratory. Our approach, or concept of operations, focuses on two simultaneous elements:

- the application throughout the Laboratory of a rigorous Integrated Safeguards and Security Management (ISSM) philosophy (that I will describe below), and
- a concentrated effort to reduce and manage our classified security assets.

At an institutional level, ISSM is evidenced by the deployment throughout the Laboratory of dedicated Security and Safeguards professionals, who report directly to my associate director

for Security and Safeguards. Their number-one focus is security, and each one of these experts has the ability—as all employees do—to stop work if he or she sees something that is being performed in an unsecure manner. We also have made changes so that all of our libraries that contain accountable classified removable electronic media, or ACREM (items such as hard drives and thumb drives), are staffed by trained security professionals whose sole job is security.

At the individual employee level, ISSM has led to a new set of streamlined, simplified security policies. And, importantly, we have taken steps to ensure that members of our workforce, including all new employees, are trained in our security policies and the elements of ISSM. ISSM for individual employees, in its simplest form, is a tool that enables them to work with security professionals and managers to identify potential security risks and mitigate those risks before there are any problems. It infuses personal responsibility and accountability requirements with clearly defined lines of authority both up and down the management chain to facilitate good communication of security concerns.

We have not only improved our policies and our security philosophy, but we have taken significant, concrete actions to reduce our risks that have made the Laboratory more secure. We have reduced our holdings of Accountable Classified Removable Electronic Media, better known as “ACREM,” from nearly 12,000 items in June 2006 to around 3,900 as of the end of August 2008. Reducing ACREM decreases the opportunities for both inadvertent and malicious activity and loss. We have accomplished this through a combination of destroying ACREM that is no longer in use and migrating significant portions to our classified networks

for archival purposes. We have further reduced risks by requiring that ACREM be stored in approved ACREM libraries staffed by security professionals. We have taken similar steps to improve management of accountable classified documents by consolidating 19 document holding areas into a single location.

We have also made significant improvements in the classified parts arena and classified parts storage, one of the areas of concern noted in the recent GAO report. Addressing the issue of the parts themselves, we have developed a robust inventory system, and we have destroyed more than 40,000 classified parts. This represents an inventory reduction of almost 50 percent. We toured the Committee Staff through one of our materials research and fabrication facilities that undertook the important additional function of parts destruction—through grinding, melting, and physically modifying classified parts into forms that are no longer classified.

Given the nature of our work, however, it is unrealistic for us to completely eliminate classified parts, as they are essential to accomplishing our Stockpile Stewardship, nonproliferation, and other national security missions. The GAO report raised specific concerns about some of the facilities in which we store classified parts, so called “non-standard storage” of classified parts. These non-standard storage areas are all approved by NNSA and are handled as exceptions to regular, standard storage. The GAO’s recommendation, and our preference as well, is to reduce as much as possible non-standard storage at the Laboratory.

We are executing a plan to eliminate non-standard storage for classified parts altogether by July 2009. We have made progress since we started this effort in October 2007, when the Laboratory had more than 32,000 classified parts that were stored in 24 non-standard storage facilities. (It is important to understand that only 20 of these facilities are what would be considered “storage”; the remaining four facilities are places where there is ongoing work “processing” material.) As of August 2008, we had closed five non-standard storage facilities and reduced the number of parts in non-standard storage to fewer than 27,000. As the Committee Staff saw on its recent visit, these non-standard storage facilities are secure, but they require compensatory security measures that add significant additional manpower costs. Our goal is to have zero non-standard storage facilities by July 2009, with the exception of the four facilities that “process” material, versus providing storage.

The Laboratory also significantly reduced our non-accountable classified document holdings. Since 2007, we have safely and securely destroyed more than 3 million pages of legacy classified documents by conducting annual destruction campaigns. This destruction effort reduced our legacy holdings by nearly 30 percent.

At the same time that we reduced the numbers of parts, ACREM, and documents, we also set out to dramatically reduce the number of locations throughout the Laboratory where this information is stored and processed. Since January 2007, we have decommissioned 34 vault-type rooms, or VTRs, reducing the total number of VTRs from 142 to 108. This represents a reduction of more than 30 percent.

One of the ways that we have been able to reduce our number of VTRs, and a way that we believe we can make further reductions, is through further consolidation of holdings into the "Super VTRs" that I referenced in my introduction. The Committee staff saw the first such Super VTR, which incorporates lessons learned in both physical and cyber security to create a "library" staffed by trained security professionals. They are responsible for the storage and checking out of ACREM, as well as the control and maintenance of classified computer servers. The first Super VTR was opened to LANL employees in September 2007, and we have since implemented plans to construct four more Super VTRs by early 2010. This will enable us to reduce the number of Vaults and VTRs by more than 40 percent.

As these consolidation efforts continue, we instituted a rigorous annual certification process for 2008. This regimen far exceeds the DOE requirement to conduct such certifications every three years. These annual certifications include effective testing of sensor systems, validating access controls, and reviewing the effectiveness of operating policies and procedures. All these certifications are reviewed and approved by our local federal oversight office.

Many of the steps outlined above are designed to reduce the risks facing each employee that might lead to a security incident. Additionally, we have put in place aggressive measures that help counter the threat of someone trying to cause harm, or someone who may create risks through their behavior. Most notably, since 2006, we have significantly increased and sustained the number of no-notice, random searches of employees near security areas. Whereas in the past, we conducted approximately 10 random searches per day, we now conduct more than 200 per day, a level that has been sustained since 2006. Additionally, as

your staff experienced, we have significantly enhanced the requirements for individuals escorted into Vaults and Vault-Type Rooms. We now employ mandatory searches, as well as inspection of all hand-carried property (briefcases, purses, etc.) upon entry and exit. We have also limited the number of days that an individual can be escorted into a vault.

Effective in March 2007, we expanded our random drug-testing program to cover all employees and subcontractors. Under the new expanded program, there is pre-employment drug testing for all new potential hires, and we have instituted random drug testing for all uncleared employees, at a level of 20 percent per year. For those employees who hold a clearance, there is an even greater chance on an annual basis that they will be tested, as we test 3 out of every 10 cleared employees annually. In fiscal year 2008 we have conducted more than 15,000 tests. All employees who have tested positive for drug use, or who have directly refused to provide test samples, have been terminated.

One additional area where the GAO raised concerns was related to perceived weaknesses in our corrective action processes. To address this, the Laboratory put in place a Corrective Action Management Review Board for security actions, chaired by my deputy associate director for Security and Safeguards. The Board reviews each new corrective action plan to ensure that it includes an effective formal “root cause” analysis, cost-benefit analysis, and risk assessment. Prior to closure of any action, the Board reviews each closure request for adequacy, and it also conducts annual self-assessments to review closed findings to validate their effectiveness. Since this new process has been implemented, we have closed 99.6 percent of our corrective action plans on schedule.

Another critical issue raised by the GAO is whether the progress that the Laboratory has made will prove sustainable in the longer term. While I cannot predict the actions of those that come after me, I can assure you that we do not view these efforts as temporary or "one time" fixes, or things that we will walk away from after we have "checked the box." For that reason, this is an issue that I personally watch very closely, and we have worked to put measures in place to ensure long-term sustainability. These measures include a Strategic Security Improvement Plan that provides Laboratory security managers with the coordinated framework from which to maintain focus and positive momentum to achieve the goal of sustained and continuous security improvement at the Laboratory. This plan encompasses a series of overarching and integrated activities that ensures the various security improvements, modernization, and performance plans and projects referenced in this plan work in concert. The plan integrates elements that include our Non-standard Storage Implementation Plan, our Super VTR2 project plan, our Human Performance Improvement Plan, our Security Compliance Order self- assessment plan, our Material Control and Accountability Improvement Plan, and our Classified Parts Management Plan.

The concrete actions we have taken to reduce our risks, clarify security roles and responsibilities, and develop solutions to continuously improve our overall security posture are working. Our trending data indicates we are on the right track. Over the last 24 months, the Laboratory has reduced unauthorized disclosures of classified information by roughly 50 percent and is continuing to trend downward. To me, this data indicates that the entire LANL team is pulling together in the right direction.

To conclude on the physical security front, I want to emphasize that this testimony has focused on the new initiatives and efforts that we are putting in place. It's important to recognize that there are a myriad of other efforts underway that I have not outlined here. For example, one of our top priorities on the physical front—as you would expect—is maintaining the effectiveness of the high security system at our Category 1 nuclear facility. The recent DOE audit validated that we are effectively protecting this critical facility. Beyond that, we are working to destroy legacy materials, consolidate what we still require, strengthen our internal and contractor security controls and processes, improve our security training, continue the deployment of our ISSM training and, most important, assure that all of these improvement initiatives are sustained for the longer term.

Cyber security improvements at LANL

Cyber security, or information security, continues to emerge as the most challenging piece of the overall security puzzle. As I mentioned in my testimony of April 2007, cyber security was and continues to be of paramount concern. The Laboratory's cyber and information technology professionals must support a dynamic and diverse national security mission, while at the same time countering an ever-increasing and evolving threat from persistent, technologically adept adversaries who are launching constant and sophisticated attacks against our information technology infrastructure and information. For both the Laboratory—and the nation as a whole—considerable effort has been applied to addressing these issues, but much remains to be done.

From a top-level perspective, I have made cyber security a key priority, and I have restructured our organization with a new chief information officer (CIO), who reports directly to me, reflecting the importance I attach to this area. At my direction, the Laboratory has consolidated oversight of institutional Information Technology governance and portfolio management and ensured improved coordination with their physical security counterparts. The LANL chief information officer also proactively opened new lines of communication with other laboratories to receive and share critical cyber information. Cyber professionals have been embedded into the organization, with the creation of senior cyber security advisors who advise, help resolve information security issues, and provide feedback to the CIO on policy questions and implementation issues.

Also, as part of the Security Compliance Order, which I will discuss in more detail below, we have started the accreditation of our unclassified computer network—something unprecedented at this scale in the DOE Complex. We are currently in the process of this accreditation, which we expect to complete in December of this year.

The Laboratory has also taken steps to integrate and centralize administration of our information technology budget, as well as develop a consistent information technology acquisition strategy. To further enhance information security, we will now be conducting blind buys of scientific and non-scientific computer hardware, software, and services to ensure that vendors will not know the intended program or recipient.

Many of the other improvements that we have made in cyber security have enabled some of the successes noted above, such as the Super VTR. Specifically, the further expansion of the Laboratory's classified network (RedNet) to an additional 33 percent of the classified community at the Laboratory has enabled the Super VTR concept, as well as our Diskless Conversion Project.

Through the Diskless Conversion Project, we have significantly reduced the threat from a malicious insider, a solid improvement over where the Laboratory stood in 2006. The project converts single-user classified workstations to centrally managed diskless computing. When complete, individuals working in classified offices and labs will no longer have the ability to write to portable media, with all writeable media being kept in access-controlled locations. The project to reduce single-user classified workstations continues to go well, with a full 94 percent of the targeted environment converted to diskless operation. Where technological limitations have necessitated a few exceptions to this process, we have applied additional accountability and other compensating protections, including extra physical protection.

In addition to removing information storage from our users' computers, we have also implemented a number of other insider threat mitigations, including:

- identifying all USB and similar ports on our classified computers;
- implementing an approved control regime for every port on our classified systems;
- enacting a strong policy that ensures separation of privilege and responsibility for users, system administrators, and information security officers; and

- ensuring that all of our server cabinets are now securely locked and accessible only under a “two person rule” or through an accountable key control system.

The GAO also called attention to the number of foreign nationals on our scientific staff and their access to our unclassified computer systems. The Laboratory is putting in place a series of controls that will be fully implemented in early 2009, which will improve the control and access to our unclassified computer networks by our foreign national employees. The plan includes a blended suite of controls to include physical barriers, software controls, and remote monitoring. Through these system upgrades, we can maintain the valuable scientific contributions made by our Laboratory employees who are foreign nationals, but also provide a higher level of cyber security as recommended by the GAO.

Security Preliminary Notice of Violation and Compliance Order

As a result of the October 2006 security incident, with which this Committee is familiar, the DOE issued a Preliminary Notice of Violation and a resulting $300,000 fine to LANS, LLC in July 2007. In addition, the Department of Energy required completion of a range of compliance order actions. Since then, the Laboratory has moved aggressively to implement all requirements of the Order.

This Compliance Order, the first of its kind in the Complex, includes 14 individual actions with due dates that started in August 2007 and the final deliverables due this December. Our compliance order efforts are being handled directly out of my office by a project leader who reports to me. We have completed 12 of the 14 actions, including many actions described

above. The remaining two involve the accreditation of the LANL classified and unclassified systems that we are on track to complete by December 12, 2008.

Planning for the future cyber threats

Security threats in general are never static, and this is especially true of cyber threats that are constantly and rapidly evolving. All of the national laboratories are taking this challenge seriously and are applying their best research and development efforts to help address this national security issue.

LANL is developing and adopting new technologies beyond diskless computing. One new technology is called Glove Box Computing, referring to the analogous way we ensure complete physical separation of nuclear material from the individuals manipulating it. This new networking concept will form the backbone of our efforts to separate certain functions and associated information, currently residing on our unclassified network, from the Internet. We are examining how to transfer our financial and human resource functions into this new network architecture as a start. We believe that this approach will provide a greater level of security without having to migrate all our unclassified systems into a classified computing environment.

The Laboratory has also worked to increase our communication and integration with the intelligence community. In this area LANL has:

- Increased integration between Cyber Counterintelligence and Cyber Security particularly in the areas of incident response and exchange of cyber threat data;

- Increased participation of laboratory counterintelligence in DOE initiatives to identify and assess external cyber threats;
- Increased participation of LANL counterintelligence in collaboration with the U.S. intelligence community;
- Increased operational collaboration between LANL counterintelligence, cyber security and the Federal Bureau of Investigation;
- Invigorated cyber counterintelligence awareness by the involvement of laboratory subject matter expert staff in briefings and solutions to mitigate external threats (e.g., foreign laptop travel program, awareness briefings coordinated through the CIO's office to different Laboratory groups including senior managers, cyber security technicians and systems administrators, among others); and
- Developed and implemented technical tools to better monitor Laboratory networks and analyze collected network data.

There is still more that can be done especially if efforts are combined with a coordinated and more robust national strategy to address the increasing virulence of cyber threats, both domestic and foreign, to the nation. Nevertheless, we are making steady progress in this area at the Laboratory.

It is important to emphasize that LANL is not doing this work alone. We leverage formal and informal partnerships with industry and other elements of the government to adopt the best technology, and make substantial technology contributions such as the Glove Box Computing and Threat Resilient Networks that I have just described.

LANL faces significant external cyber security threats

Even with the progress the Laboratory is making in both physical and cyber security, our defensive efforts must now start to evolve in a more cohesive and organized fashion. This higher level of organization is needed because, as the Laboratory director, I must ensure that I properly prioritize my security mitigation priorities against our greatest areas of risk. For example, all of the Laboratory's systems connected to the Internet sustain thousands of penetration attempts daily by extremely sophisticated external parties.

Because of the assortment of unclassified and classified computer systems that we maintain to support the Laboratory's mission requirements, my security team is analyzing our risks and making judgments on how best to allocate our cyber resources. Our classified resources are our highest priority, but the unclassified networks are the backbone of our operations and communications activities. Developing protection solutions that both manage risk and allow user functionality for the execution of daily operations is crucial.

It is this need for unclassified functionality that drives my belief that no individual laboratory alone is going to have the needed resources to handle this evolving threat. As I mentioned earlier, our unclassified systems are being attacked thousands of times a day, and we have developed some fairly advanced technologies to defend ourselves, but my resources are not limitless.

I believe that total coordination across the DOE complex vastly increases both the knowledge base and resource pool to draw from. The NNSA laboratories, through the

auspices of NNSA headquarters, have already established communications protocols to inform each other of cyber security issues at a particular laboratory. This level of collaboration, along with greater collaboration with the intelligence community, is a microcosm of a larger effort that needs to be harnessed into a truly national effort.

Cyber incidents occur across the federal government and across our country. Our information networks are indispensable to our daily activities, and (as we have all seen in countless media stories) the scope and breadth of cyber intrusions are accelerating. I believe that the national laboratories can be a valuable resource to the nation because of our unique cyber capabilities, but this needs to be part of a high-level federally coordinated effort.

Conclusion

Mr. Chairman, during the two years since I arrived at Los Alamos National Laboratory, security—both physical and cyber security—has been my priority. The Laboratory has made significant progress in enhancing our security posture. At the same time, the findings outlined by both the GAO and the HSS identify areas, particularly in cyber security, where the Laboratory needs to continually improve against adversaries who are constantly probing and adjusting to penetrate our defenses. As your staff has seen, we have developed and are implementing corrective actions for the identified issues as a result of these findings. Lastly, I am encouraged by the fact that both the GAO and several of the HSS ratings do mention that we are making substantial progress as we continue to do our utmost to secure the nation’s secrets.

The improvements made at the Laboratory link directly back to the attitude of our employees. There is very little tolerance now among the workforce for co-workers who are not security conscious. In addition, the thinking behind making classified information more secure (but at the same time accessible so that we can execute our mission requirements) has led to our dramatic reduction in Vault Type Rooms and the development of the Super Vault Type Room concept. Both are positive examples of how the Laboratory recognizes the need to change and then develops innovative solutions to take it a step further.

However, even with what has been good progress, Mr. Chairman, the danger posed by cyber threats is now our primary threat. With the laboratories and the Department working together, our coordinated and pooled resources and technical capacity will be formidable in defense of this nation. Building on these current collaborations within NNSA, with other federal agencies, laboratories, and the private sector, offers the best path forward to meet this daunting challenge.

Mr. Chairman, I thank you and the members of the Subcommittee for allowing me the opportunity to testify today. When we move to the closed session of this hearing I would like to outline in greater detail the types of organized cyber threats that the Laboratory has faced, coupled with our responses, and to discuss in greater detail our defensive capabilities. Thank you again, Mr. Chairman, and I would be happy to answer any questions.