TESTIMONY OF MICHAEL ANASTASIO
BEFORE HOUSE ENERGY & COMMERCE COMMITTEE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
JANUARY 30, 2007

Executive Summary

Michael Anastasio has served as Director of Los Alamos National Laboratory and President of Los Alamos National Security, LLC ("LANS") since June 1, 2006, when LANS began operating the Laboratory under a new management contract. Dr. Anastasio came to Los Alamos because it is an institution that is vital to the national security of our country. From ensuring the reliability of our nuclear weapons stockpile to developing solutions to help combat nuclear terrorism, the people at Los Alamos are a unique national scientific and engineering resource.

Last summer, Los Alamos National Laboratory suffered what LANS considers to be a very serious security breach. Dr. Anastasio is deeply troubled that a subcontractor employee with a high-level security clearance willfully circumvented DOE and Laboratory policies and procedures and removed classified material. At the same time, he is equally concerned that management systems failed to prevent this security failure.

Both the LANS Board of Governors and Dr. Anastasio, while cooperating fully with a number of government investigations, directed an immediate series of actions in response to this incident that included:

- halting classified scanning activities;
- bringing in independent security experts from the LANS parent organizations to assist in thoroughly understanding and responding to this incident;
- eliminating, disabling, and controlling high risk ports on our classified computer networks;

- revising and tightening Laboratory policies on escorting;
- creating a new cyber-security organization reporting to the Director;
- increasing physical searches across the Laboratory;
- enhancing existing drug testing policy; and
- accelerating the review and modification of physical and cyber security policies and procedures.

Following these immediate actions, Dr. Anastasio disciplined or took administrative action against 24 employees for their roles in this security violation and ordered the termination of all subcontracts with the company involved in this incident.

The LANS goal of transforming the Laboratory is much broader than these specific corrective actions. LANS is -- and has been since June 1 -- working to break down local organization control and interpretation of policies and procedures. LANS is working hard to make sure that all employees, Lab-wide, interpret and apply policies, including those relating to security and safety, in a consistent, enterprise-based manner.

When LANS was awarded the contract, they knew LANL had problems on many levels that must be addressed. The LANS team is actively engaged in both determining the true depth of those problems and mitigating them in a timely manner. In this effort, Dr. Anastasio is greatly aided by the oversight of the Board and the resources of the four LANS parent organizations. This incident highlighted the need to move even more aggressively. They regret that time did not permit LANS to progress far enough in the cyber security area to prevent this incident. Dr. Anastasio and the LANS team have achieved many measurable improvements to date in response to this incident, but readily admit much more needs to be done and they have set about doing them.

Introduction

Chairman Stupak, Ranking Member Whitfield, and members of the Subcommittee, I appreciate the opportunity to appear before you this morning.

My name is Michael Anastasio, and I am the Director of Los Alamos National Laboratory in New Mexico as well as President of Los Alamos National Security, LLC. I have served in this capacity since June 1, 2006, when Los Alamos National Security, or "LANS", began operating the Laboratory under a new management contract, following more than 60 years of management by the previous contractor. Although I am new to Los Alamos, I have served our country for more than two decades working in the national security arena at Lawrence Livermore National Laboratory in California where I served as Laboratory Director prior to my arrival at Los Alamos.

I came to Los Alamos because it is an institution that is vital to the national security of our country. From ensuring the safety and reliability of our nuclear weapons stockpile to developing solutions to help combat nuclear terrorism or for energy security, the people at Los Alamos are a unique national scientific and engineering resource. It is this science and engineering talent that made my decision to go to Los Alamos easy when I was asked to lead the LANS bid team almost two years ago.

The same is true for my management team who decided to join me in bringing their experience and expertise to the Laboratory. Likewise, the four parent companies that comprise LANS have a demonstrated record of experience and accomplishment throughout the Nuclear Weapons Complex and commercial industry. As we move forward addressing operational challenges, we have focused on aggressively implementing systematic corrections that are fully integrated with behaviors.

It is my belief that many of the past problems at Los Alamos were never fully rectified. Many corrective actions were formulated and implemented at the local organizational level, without clear and consistent implementation across the entire Laboratory. That approach continues to leave the Laboratory vulnerable to the reoccurrence of security problems that are the basis for this hearing. A highly experienced management team is applying institution-wide standards through an integrated management philosophy. Coupled with oversight by and reach back to our LANS parent organizations, we have and will continue to address those problems in a manner that engages and holds employees accountable at all levels of management in the very serious business of national security.

Mr. Chairman, shortly after LANS took over management, Los Alamos National Laboratory suffered what I consider to be a very serious security breach. I am deeply troubled that a subcontract employee with a high level security clearance willfully circumvented DOE and Laboratory policies and procedures and removed classified material. I am equally concerned that we had inadequate management systems that failed to prevent this security failure. Both my Board of Governors and I directed an immediate series of actions to attack this incident that included:

- cooperating completely with Department of Justice and Department of Energy investigations triggered by this serious event;
- bringing in independent external security expertise from the LANS parent organizations to assist me in thoroughly understanding and responding to this incident;
- eliminating, disabling, and controlling high risk ports on our classified computer networks; and
- accelerating the review and modification of our physical and cyber security policies and procedures.

The immediate actions that were initiated helped stabilize the uncertainty surrounding this incident which then allowed me to focus on the accountability aspect of what occurred.

Later in my testimony, I will describe in detail the specifics regarding accountability for this incident over and above the ongoing law enforcement action being taken in connection with the subcontractor employee who removed classified information. In summary, I personally evaluated the acts or failures to act that directly or indirectly contributed to this incident and found three key failures:

- failure of the escorts to properly perform their duties by maintaining 100% visual and auditory control over the subcontractor employee;
- failure to limit the subcontractor employee's physical access to only that hardware essential for her to complete her task; and
- failure to uniformly address risks posed by open USB ports in both classified and classified/unclassified mixed environments.

In the following sections I will discuss these and other factors and how we are addressing these issues through corrective actions.

I have held 24 employees accountable for individual failure to fully execute assigned responsibilities which contributed, directly or indirectly, to this security violation. I also ordered the termination of all Laboratory subcontracts with the company that employed the individual who removed classified information. However, holding these individuals accountable will not in itself provide me with an adequate path forward, because as we have seen in the past at Los Alamos, just dealing with poor employee behaviors in isolation did not sufficiently address the underlying problems. Our path forward will be to break down local control of the policy and procedure process and to make sure that all employees follow a common set of goals and expectations related to

security and safety that apply across the nearly 40 square miles of laboratories and facilities that we manage as Los Alamos National Laboratory.

Completing such a shift cannot be accomplished quickly. However, LANS is bringing a completely different approach to management and oversight that we believe will work. There is oversight by the Board, as well as resources through the parent organizations, that are a great asset to me and my efforts. Having these additional resources, an expert management team, and a clear understanding of what has not worked in the past gives me the unique opportunity to effectuate successful change at the Laboratory. Moreover, the Board is committed to assisting me by importing best practices and seasoned personnel from their successful operations at other DOE sites.

LANS Approach to Enhanced Security

As the leader of the LANS team, I am acutely aware, as is my Board of Governors, that the Laboratory management contract was placed out for bid in large measure because of past security and safety incidents. It was this understanding, confirmed by what we were able to learn during the transition process, which caused me to take immediate actions to begin the enhancement of our general security posture when I took over as Director on June 1, 2006. At that time I created a Chief Security Officer position that reports directly to me, elevated the head of safeguards and security to the level of Associate Director, and created a more clearly defined accountability structure for cyber security.

Additionally, I split the highly classified Dynamic Experimentation (DX) Division into two separate divisions to decrease the span of control and to increase managerial oversight. I also installed completely new leaders into each element of the

new organization. I took these actions because DX Division had a history of safety and security problems that I dealt with by planning actions during transition and acting on them on day one of contract assumption (June 1, 2006).

We started that process during transition and expected it would continue well into the first year of our contract management. During transition, we became aware that there were problems in the cyber security operations, the majority of which centered on a lack of consistent policies and procedures, uneven adherence to physical security procedures, and a lack of adequate funding to substantially complete our diskless computing project.

The Department of Energy's Inspector General indicated that the "root cause" of this incident was inappropriate actions of an insider. I agree with this assessment but it is only part of the story. The fact that a subcontract employee was able to commit this act without detection confirmed one of my primary concerns. This incident exposed a problem not only involving employees' attention and attitude, but also the Laboratory's reliance on a very complex and confusing set of cyber security policies and procedures that made it difficult for the employees to make good, immediate judgment calls.

It is evident that in this current incident many judgment calls were incorrect. This will result, as I mentioned earlier, in my holding twenty-four Laboratory employees accountable for their mistakes. Yet a significant contributing factor, and one I considered in determining an appropriate response to these mistakes, was our failure to provide these employees with clear, current, and effective policies, procedures and training that enabled them to comply with requirements while getting their jobs done.

Are We Really Different?

At the time of the contract award, LANS immediately implemented self-governance oversight as described in our proposal to NNSA. Our implementation of the parent organization oversight function consists of the Board of Governors and its Committees; parent organization functional management assessments; and AIM (Assess, Improve and Modernize) teams.

As Laboratory Director, I report directly to an independent, very actively involved Board of Governors, established by the four LANS parent companies (Bechtel National, the University of California, BWX Technologies, and Washington Group International). This Board has access to the substantial technical, management and operations expertise of those organizations, including security expertise, which we have already drawn upon. The Board was originally created with six committees and as a result of this security incident, the Board has created a new seventh committee, the Committee on Safeguards and Security. The newly formed Committee of the Board of Governors will focus solely on oversight of Safeguards and Security, including cyber security, and will report directly to the Board Vice Chairman. By creating this new Committee, LANS has elevated the urgency of oversight and accountability for security activities.

The LANS governance structure was created to capitalize on the individual strengths of the partners, further strengthened through the involvement of outside experts in areas relevant to the Laboratory's operations. The Board has eleven governors, six from the member organizations, who collectively comprise the Executive Committee, and five independent expert members.

Functional assessments are performed in all areas of the Laboratory and are conducted by parent organization experts from corporate offices and other DOE and NNSA sites managed by the parent companies, as well as other subject matter expert consultants. These teams of external experts are a critical element of our oversight and a significant departure from how oversight was conducted in the past at Los Alamos National Laboratory.

Another category of oversight is in the form of what were referred to in our contract proposal as Assess, Improve and Modernize or "AIM" Teams. AIM Teams will assess and improve critical areas of concern, such as those identified in the area of cyber security. AIM Teams, which have been used successfully by the LANS industrial partners at other sites, will generally come from outside the Laboratory – from the parent organizations and other DOE and NNSA sites managed by the parent companies. These AIM Teams are a critical method for ensuring that corrective actions are implemented effectively and ensure that the Laboratory is staying ahead of the ever changing risk environment. In fact, as explained below, an AIM team was dispatched soon after the recent security incident.

Summary of the Incident

On October 17, 2006, while serving a search warrant related to a drug investigation, officers of the Los Alamos County Police Department seized three computer "thumb drives" from the Los Alamos residence of a former Laboratory subcontractor employee. These are the sort of tiny memory devices that can be carried on a key chain. Another resident of the trailer was the target of the drug investigation.

Two days later, on October 19, 2006, the Police Department discovered on one of the thumb drives a document with classified markings. The police immediately referred the matter to our Laboratory's associate directorate of safeguards and security, which assumed custody of the thumb drives. Our review of the thumb drives revealed that they contained numerous Laboratory documents some of which were marked as classified.

The Los Alamos Site Office of the NNSA authorized the Laboratory to notify the Federal Bureau of Investigation (FBI), which on October 19, 2006, assumed responsibility for the investigation. The next evening, the FBI searched the subcontractor employee's residence and seized a tote bag containing 228 sheets of printed paper, some bearing classified markings. The person targeted by the drug investigation said that the documents and thumb drives belonged to the subcontractor employee.

A complete review of the contents of the thumb drives and the tote bag revealed copies of Laboratory documents, some of which are classified documents, which we determined to have originated in a vault-type room in the Laboratory's Dynamic and Energetic Materials Division (one of two new divisions created from the reorganization of DX division).

At the time of the incident, the subcontractor employee held a Q-level security clearance, which was issued to her by the Department of Energy. For a year, from August 31, 2005 until August 31, 2006, the subcontractor employee scanned and indexed documents in the vault-type room as part of a project to preserve and archive old technical documents. For that assignment, she received appropriate training and

acknowledged security requirements of the applicable security plan for the vault in which she worked.

The subcontractor employee had previously worked at Los Alamos as a student from June 5, 2001, until April 29, 2005, when she voluntarily left her student position and began working for a subcontractor to the Laboratory. From April 2005 until September 2005, she trained with that subcontractor and archived classified documents for a different Laboratory organization prior to moving to the scanning operation at issue. We have no evidence that she acted inappropriately during any of her earlier work assignments at the Laboratory.

A Laboratory-led team of experts, including nuclear weapons experts, conducted a preliminary damage assessment of the information that was found on the thumb drive and elsewhere at the trailer. I am more than willing to discuss the details of the assessment with you in a closed forum, but am unable to address those issues in an open forum due to security concerns.

The FBI conducted a forensic study of both the thumb drive and the work stations in the vault-type room where the subcontractor employee worked. This review revealed that the thumb drive was inserted into a work station, that a large print job was sent electronically to the vault printer adjacent to her work area at 2:00 p.m. that same day, and that the thumb drive was removed from the same work station at a later date. Forensics could not provide other details such as the number of times the thumb drive was inserted and removed during that period.

The FBI has met with the subcontractor employee on two separate occasions and it is our understanding that the FBI intends to conduct additional follow-up

interviews. We anticipate that the FBI will share relevant information regarding their investigation which would be relevant to our security enhancements.

We also understand that the subcontractor employee stated that her motivation for removing the classified media and documents was to help meet a work deadline that she was behind in fulfilling. Forensic analysis conducted to date is consistent with this claim.

Since the incident on October 17, 2006, we have worked closely with the DOE, the Los Alamos Site Office of the NNSA, the Los Alamos Police Department, and the FBI to share information, examine forensic evidence, and conduct personnel interviews. The extraordinary level of collaboration between these agencies allowed us to quickly grasp the scope of the problem, take effective immediate corrective actions, and pinpoint the most serious security policies in need of urgent work.

Cyber & Physical Security Corrective Actions: Immediate and Longer-Term

Following notification of the incident, I quickly directed a series of short-term precautionary actions within the Laboratory, based on the limited information that we had at the time. These included:

- halting all classified scanning activities;
- reviewing and enhancing the policy prohibiting the introduction into security areas of non-government owned memory devices (such as iPods, camera memory cards, and thumb drives);
- reviewing and enhancing policies and procedures relating to escorting and operations in vault-type rooms; and
- physically disabling all unnecessary high risk computer ports.

After my team had more time to analyze the incident, I instituted a comprehensive and long-term set of actions related to cyber security. As a starting point,

I assigned a group of key managers to evaluate issues associated with the immediate steps taken to date and to develop policies and procedures that are sustainable in the long-term.

Disabling Classified Computer Ports

I directed Laboratory managers to ensure that the ability to download classified material to unauthorized devices had been physically disabled. Although many of our ports in classified computing work areas have been disabled using software, we added an additional security layer by physically disabling more than 5,800 USB ports and more than 1,400 fire wire ports. Furthering our efforts, we have recently identified other ports, subject to the most recent DOE cyber security guidance, and have taken steps to eliminate, disable, control or severely limit and manage access to those ports.

Suspended Classified Scanning Activities

Also, as I mentioned earlier, we temporarily suspended all classified scanning activities. During this pause, I ordered a detailed evaluation of the policies and procedures governing all scanning activities prior to each activity being restarted. We are not aware of any similar problems or issues with the other scanning activities.

Review Subcontractor Security

To ensure proper communication about, and compliance with, security procedures among our subcontractor workers, I directed the Laboratory's procurement organization to conduct a review of all subcontracts to ensure that required security provisions had been properly flowed down. In addition, I directed the Laboratory's procurement organization to meet with representatives from Laboratory subcontract companies to ensure a common understanding of security requirements and expectations. The Laboratory's procurement organization instituted an ongoing process to verify that

contract companies are aware of and in compliance with security related contractual requirements, such as the creation and implementation of compliant Operational Security, or OPSEC, plans.

Security Escorts

In addition, we scrutinized the policies and procedures for escorting workers and visitors and for the operation of vault-type rooms to ensure there are clear directions in place for all Laboratory employees providing access to these secure areas. For example, revised escort policies now require an escort to search the belongings of the person he or she is escorting prior to entering and exiting a vault-type room. In addition, escort/security plans are now required in instances where an individual will be escorted for more than ten days. These policies will continue to be reviewed and enhanced to ensure that they contain clear requirements so that employees may fully understand what is expected of them.

Employee Training and Communications

The Laboratory is also reviewing and will enhance its training and overall communications to ensure security requirements are clearly understood by all employees and that issues are elevated to and addressed by management. To that end, I asked each employee to personally review cyber security and physical security plans and procedures for their work areas and provide feedback through their management chain for appropriate action.

New Cyber Security Organization

I determined that the current organizational structure for cyber security was inadequate and lacked sufficient functional integration needed to manage the complex cyber issues at Los Alamos. For this reason, I created a new cyber security office charged with integrating and streamlining our cyber security policies and procedures, integrating implementation of those policies and procedures across the Laboratory, formally validating compliance with those policies and procedures, coordinating what types of technologies will be approved for configuration into our existing systems, and developing an emerging technology risk program. Each of these areas are critical for the Laboratory to develop a high fidelity cyber security program appropriate to the unique challenges of operations at the Laboratory and responsive to new technologies that may pose risks to our systems in the future.

Increased Physical Searches

Preventing this type of incident poses physical security challenges as well. I directed that the Laboratory security force enhance our physical search procedures. We increased the average number of employee searches to more than 100 per day. It was important to step up physical searches as an added deterrent. These random searches will complement the new escort search requirement for classified vaults and will help us in detecting those individuals who might attempt to repeat the actions associated with this security incident.

Enhanced Drug Testing Policy

As a result of the many reviews this incident has produced, I also decided to accelerate the planned enhancements to our existing substance abuse policies. I

enhanced the drug testing policy for all Laboratory direct employees and onsite subcontractors. All new employees and onsite subcontractor employees will be subjected to drug screening prior to being hired. Initially, I have directed that we randomly screen a minimum of 20% of the entire workforce (badged employees and onsite subcontractor employees) on an annual basis.

Accountability

Termination of Subcontractor Contracts

As identified by the various internal and external investigators assigned to this matter, the root cause of this security incident was the willful violation of policies and procedures by a subcontractor employee. The subcontractor employee was laid off by her employer at the completion of the scanning project and before her misconduct was discovered. I also ordered the termination of all Laboratory subcontracts with the company that employed her. Further, I instructed the Laboratory's Human Resources Division and Security Division, working with the local NNSA office, to ensure that the subcontractor employee does not gain access to Laboratory property either as a direct employee or subcontractor.

Employee Disciplinary Actions

With respect to Laboratory employees, the disciplinary measures I have imposed are a direct result of a series of security system weaknesses and procedural violations that culminated in a failure to prevent or detect the subcontractor employee's unacceptable behavior.

Disciplinary actions included the removal of three employees from their cyber security management positions. Both the security responsible line manager and the

project manager received written reprimands and unpaid two week suspensions. In addition, seven other Laboratory employees received written reprimands and eight received written counseling. For five of my most senior managers, I utilized a guidance tool that was very effective during my tenure at Lawrence Livermore National Laboratory. This tool, a Memorandum of Expectations, clearly outlines my security expectations of them and addresses their roles and responsibilities related to their individual corrective action plans for physical and cyber security.

The twenty-four personnel actions I executed are commensurate with the security violations that occurred. I also know that both my team and I are ultimately personally responsible for ensuring that lapses like this do not reoccur. That is the same message that the LANS Board of Governors has also delivered to me personally. They also provided these assurances to the Secretary of Energy as well. It is a message that we all understand.

LANS Commitment

As I have said before, the Laboratory's long string of security lapses was a significant consideration in the Government's decision to re-bid the management contract at the Laboratory. I can assure you that I am quite aware of the fact that I and my team will be judged against how able we are to address the underlying causes and failures that lead to this type of incident at the Laboratory. We all understood through the bid, transition, and managerial assumption process that the Laboratory was in significant need of change across all its operational areas, but in particular security.

When we bid on the Los Alamos contract, the LANS team believed that most operations at the Laboratory, and in particular security, were being hampered by

enormous spans of control, a lack of coordinated and integrated policies and procedures, rapid advance in technology-driven security risks, and a workforce that had become focused on compliance rather than proactively "owning" solutions themselves.

When we formulated our management plan and structure during the bid and transition process, we did not look to create anything overly complicated because we believed that what was needed more than anything else was clarity and simplicity. Our original plan envisioned a one-year timeframe during which we would develop comprehensive and integrated operating procedures that would then be flowed down through all the Laboratory's organizations, and we were hard at work executing that plan when this incident occurred.

Solution and Path Forward

From my meetings with several of you and with Subcommittee staff, I know that, very understandably, there is a strong desire for a big, dramatic—even revolutionary—change to fix the problems, security and otherwise, at Los Alamos. I will tell you, however, that I do not believe that such a silver bullet exists.

When the LANS team evaluated and bid on the contract, we concluded that what we were inheriting was a great Laboratory with brilliant minds, but an organization that had grown up in secrecy and necessary compartmentalization. As a result, LANL became a less cohesive laboratory and more a set of independent organizations, each with its own manner of operations and expectations.

Clear Lines of Management Authority

Our solution to this—which I do believe is revolutionary within the confines of the Laboratory, and has not been done previously—is to put in place clear

lines of authority, the right leadership, manageable spans of control, and involvement of workers in implementing security and safety in their workplace. All these steps integrate separate organizations into an institution that can work even more effectively as a team to solve the nation's national security challenges. Said another way, I have described a "shared fate" that includes myself, as Laboratory Director, through all levels of the workforce, and including the community to make the great strides expected of us for the benefit of the nation.

To ensure that all levels of the Laboratory receive and understand what is being asked of them, I am utilizing my new management team to ensure proper communication. This is an approach that worked for me as Director of Lawrence Livermore National Laboratory. At Los Alamos National Laboratory, my senior managers now are able to better focus on their areas of responsibility and I am now better positioned to hold my entire team accountable.

Continue the Walk

While there is no immediate panacea, the actions LANS is currently taking and initiatives I have put in motion will put the Laboratory in a position where it can better anticipate risk and prevent incidents. I have concluded that we need to vigorously attack this issue on five fronts: processes and policies, organization, infrastructure, tools, and people.

Interim Cyber-Security Organization

I have said much about the ambiguity of policies, roles and responsibilities, and the disparate implementation of same. I am committed to resolving those issues. I have formed an interim cyber security organization that centrally aligns

cyber security policy and implementation responsibilities in one organization that reports to me. For the long term, my Chief Security Officer will recommend to me a permanent "steady state" organization that optimizes the Laboratory's information architecture and systems in a manner that best promotes integration with the mission and physical security requirements.

In developing such recommendations, the Chief Security Officer will take into account the findings and recommendations of the Office of Inspector General's Special Report to the Secretary as well as the observations and recommendations of the LANS Board of Governor's review which utilized a team of experts from the LANS parent companies. Aside from the implementation of a new cyber security organization, the Laboratory has carefully considered all Office of Inspector General and Board of Governors' recommendations and is implementing corrective actions that are aligned with recent guidance on cyber security from the Deputy Secretary of Energy.

The expected outcomes of the interim cyber security organization and, ultimately, the permanent organization are as follows:

- roles and responsibilities are clearly defined;
- policies are compliant with DOE requirements;
- policies are implemented in a consistent manner by line management with worker involvement;
- certification and self assessment of implementation are centralized at the institutional level and not left to individual organizations; and
- cyber security implementation is integrated with other security requirements.

Compliance with Recent DOE Cyber Security Guidance

I believe that the recent guidance from the Deputy Secretary of Energy will help drive Los Alamos and other DOE sites to advance engineered fixes and

anticipate emerging technological risks. On January 26, 2007, a federal audit team reported that "after a 100 percent review and validation, all LANL vaults and vault type rooms have me[t] the requirements for enhanced port controls on classified computers per the DOE Deputy Secretary's memorandum of November 8, 2007." Our initial efforts, which were launched in advance of the specific guidance, did not sufficiently encompass the broad array of computer ports in the LANL work environment. Through hard effort by my management team and the efforts of our dedicated workforce, we now comply with the guidance. I view this as a solid foundation from which to build sustained compliance and continuous improvement.

Outside Cyber Security Experts

Clearly, the organizations tasked with responsibility for cyber security and our employees need to be equipped with the best available tools to counter security risks. To that end, I have tasked my Chief Security Officer to formulate a team of outside industry and government cyber security experts who are conducting an examination and evaluation of technology evolution for the purpose of better anticipating and minimizing future cyber security risks. That team will recommend to me a strategy and approach for staying ahead of such technological risks that also face the Nation as a whole.

I am mindful that less than carefully considered "fixes" can have unintended consequences. At a complex laboratory such as Los Alamos, this is not a trivial matter. The information technology environment is perhaps the most dynamic management challenge to the Laboratory since it is inexorably coupled to the productivity and health of the Laboratory. An obvious lesson learned from this particular security incident is that cyber security must be an integral part of the Information Technology (IT)

environment as information architecture evolves--that is, cyber security must be a design criteria for new systems, as opposed to being retrofitted after the fact.

Vault Type Room (VTR) Security Pilot

I am currently planning a pilot project to develop and demonstrate our concept, including the configuration of our vault type rooms. This approach will enable us to apply the best ideas and closely monitor the results in a test environment before applying them Laboratory-wide.

The concept, which we call the "Super VTR Concept", is built on several key features that address the five thrusts I discussed earlier—processes and policies, organization, infrastructure, tools, and people.

First, we will consolidate and uniformly control the use of classified information while using technology to efficiently and effectively enable authorized, programmatic access. The consolidation will address a major challenge to cyber security at Los Alamos, which is the large number of vault type rooms distributed across the Laboratory.

Second, the Super VTR will build upon the significant investment by the Laboratory in the Red Network expansion project that provides ubiquitous classified network access from individual work stations to the Super VTR. Third, the Super VTR will be designed to accommodate the broad scope of classified information that the Laboratory utilizes in the performance of its work.

Fourth, the Super VTR will have additional cyber and physical security requirements designed into its operation. Fifth, The Super VTR will be staffed with a cadre of trained, professional security staff who report to a central organization in support

of the programs that utilize the VTR. In addition, we will monitor "culture" issues by monitoring human performance through the use of modern management systems and metrics.

The Super VTR pilot will serve as a platform from which to launch the Laboratory from a base of competent and compliant cyber security operations to a new environment for secure cyber security operations. That new environment will be at the leading edge helping to define the future and not just react to it.

Performance Based Leadership

To raise the bar across the Laboratory, the LANS team brought with it Performance Based Leadership which is a systematic approach to coaching and cascading management values through all levels of management. My team has been trained in this approach and I have accelerated the schedule so that we will have completed all levels of management by the end of this Fiscal Year. To be credible leaders, my entire management team must model the values and expectations that are expected from the workforce.

Other Initiatives

The LANS team is embarked on other initiatives to implement best industry practices to improve all aspects of operational performance. One of these initiatives, Human Performance Improvement (HPI), draws directly from success in the nuclear power industry, which dramatically reduced the number and severity of adverse events through a better understanding of human fallibility. Developed by the Institute of Nuclear Power Operations (INPO) and now successfully implemented in a number of private-sector applications, HPI focuses on developing systems and processes that

minimize the incidence of human error and mitigate the consequences of error when it inevitably occurs. As discussed above in the context of the Super VTR concept, I will utilize HPI in the management of this critical pilot.

Let me briefly elaborate on that concept. Systems such as procedures, policies, equipment operation, and organizational structures have the equivalent potential to provoke human error as to eliminate or mitigate the consequence of error. Therefore, the management of these systems requires a two-fold approach: (1) identifying and correcting weaknesses in systems that provoke error; and (2) building robust and redundant defenses within systems to mitigate against human fallibility.

It is my intent to utilize the Super VTR pilot to introduce error precursor measures that help management anticipate potential issues and, more importantly, help employees succeed by eliminating or modifying error prone policies, processes, and systems.

Conclusion

To conclude, I want to reiterate the high degree of rigor, resolution, and urgency that are typical of this team since the beginning of transition. We knew we had problems to address at the Laboratory, and we are engaged in both determining the true depth of those problems, and mitigating them in a timely manner. This incident highlighted the need to move even more aggressively. I regret that time did not permit us to be sufficiently mature in our cyber security posture to prevent this incident. However, I am proud of the effort we have brought to bear and the results we have achieved to date in response to this incident. We took immediate action to close potential security gaps as quickly as possible. I also want to raise this caution: we are aggressively reducing

security risks, but we cannot guarantee zero risk as that would necessarily prevent us from performing our mission.

All of us who care deeply about national security must continue to work together to both protect our nation's most sensitive secrets and allow our nation's best scientists to do their essential work for our future. If I can leave you with one message – it would be that the LANS parent organizations, the LANS Board of Governors, my leadership team and I will do all within our power to make the Laboratory the model and standard for security and safety excellence within DOE/NNSA while consistently reaching for world class research and scientific excellence.

I also would like to emphasize to you today the dedication of our employees to the crucial national security work of the Laboratory. The only way to truly understand what we do is to come and visit the site. I would like to personally extend an invitation to each of you to visit the Laboratory and to meet our employees who are dedicated to certifying our nation's nuclear weapons, meeting the challenges posed by weapons of mass destruction, and conducting research in energy, biology, and environmental science to address national priorities.

Mr. Chairman and Members of the Subcommittee, I ask that my full remarks be entered into the record, and I would be happy to answer any questions.

Thank you.