A REVIEW OF CONTINUING SECURITY CONCERNS AT DOE'S NATIONAL LABORATORIES

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

SEPTEMBER 25, 2008

Serial No. 110–152

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
63–238 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chair
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
DAVID L. CAVICKE, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

BART STUPAK, Michigan, *Chairman*

DIANA DeGETTE, Colorado
CHARLIE MELANCON, Louisiana
Vice Chairman
HENRY A. WAXMAN, California
GENE GREEN, Texas
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
JAY INSLEE, Washington
JOHN D. DINGELL, Michigan *(ex officio)*

JOHN SHIMKUS, Illinois
Ranking Member
ED WHITFIELD, Kentucky
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas *(ex officio)*

CONTENTS

A REVIEW OF CONTINUING SECURITY CONCERNS AT DOE'S NATIONAL LABORATORIES

THURSDAY, SEPTEMBER 25, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:09 a.m., in room 2123, Rayburn House Office Building, Hon. Bart Stupak (chairman of the subcommittee) presiding.

Present: Representatives Stupak, Green, Inslee, DeGette, Dingell (ex officio), Shimkus, Burgess, and Blackburn.

Staff Present: Scott Schloegel, John Sopko, Chris Knauer, Steve Futrowsky, Joanne Royce, Kyle Chapman, Alan Slobodin, Peter Spencer, and Whitney Drew.

OPENING STATEMENT OF HON. BART STUPAK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. STUPAK. This meeting will come to order. Today we have a hearing entitled, "A Review of Continuing Security Concerns at Department of Energy's National Labs." We'll start with opening statements. I'll begin.

Today we'll hear from several independent sources about security problems that continue to plague the Department of Energy's nuclear weapons labs. We'll also hear from DOE officials responsible for the operations of the labs and then we'll hear from the lab directors who will tell us what they're doing to address the shortcomings.

The Department of Energy's nuclear weapons labs are home to some of the country's most sensitive secrets and the country's most dangerous nuclear materials. These labs—Sandia, Los Alamos, and Lawrence Livermore—employ the world's most brilliant scientific minds, but they've also been home to some very serious security breaches.

Los Alamos has historically been our most challenged of the three labs. This is the 14th hearing our subcommittee has held into security problems at Los Alamos over the past 8 years. We've also requested numerous Government Accountability Office investigations, which have resulted in countless recommendations for improvements at Los Alamos. Thankfully, the LANL has implemented several changes that appear to be improving the physical security posture. Our staff was encouraged by many of the changes they saw at the lab with regard to physical security, and these views appear to be echoed by the GAO and the Office of Inde-

pendent Oversight Reports. We remain optimistic, but guarded, that Los Alamos will continue to improve.

Unfortunately, at the same time that physical security at Los Alamos was improving, Lawrence Livermore National Lab was actually regressing. Earlier this year the Department of Energy's Office of Independent Oversight conducted a force-on-force exercise at Lawrence Livermore which, according to GAO testimony, resulted in the lab receiving, and I quote, "the lowest possible ratings for protective force performance and for physical protection of classified resources," end of quote. While we are told by lab officials that they have made numerous changes to their security force and procedures to correct the problems, we expect to learn exactly why or what led to the failures and what corrective measures have been put in place to ensure that they will not occur again.

Physical security is just one component to keeping our nuclear secrets safe. The most recent vulnerability is that a host of unauthorized sources are trying to exploit our lab's cyber networks. The Department of Energy's cyber networks are attacked millions of times each month by individuals ranging from a high school kid looking for a challenge, to the most sophisticated adversaries who are seeking very specific information.

Today, we will hear concerns about the Department of Energy's cyber security posture from three government entities.

First, the Government Accountability Office will discuss their report detailing shortcomings of the unclassified computer network at Los Alamos National Lab. Moreover, they will document how highly sensitive—but unclassified—information on the Department's network may possibly be pieced together and could become classified information which would be "a valuable target for foreign governments, terrorists and industrial spies."

Second, DOE's Office of Independent Oversight will tell us about how a small team of their cyber attack experts, known as a "Red Team," were able to hack into and gain full administrative control over two of the Department of Energy's science lab computer systems. This same team was also able to gain a foothold into part of the weapons labs computer systems.

Third, we will hear from the DOE's Inspector General, who will discuss their recent report outlining the vulnerabilities in the Department's unclassified cyber security program and its need to improve management and controls. They will document that "since the end of fiscal year 2007, the Department has experienced a 45 percent increase in reported cyber security incidents." In addition, we will hear from the DOE's Associate Director of Counterintelligence that DOE networks have picked up an increased tempo of potential adversarial activity, and in some cases, sensors have documented "well over 400 million such indicators of hostile activity every month."

Make no mistake about it, cyber security at our Nation's energy labs should be of paramount concern to Congress and the American public. The sophistication of our adversaries when it comes to cyber attack is significant. But if the Department of Energy, and all the Federal Government for that matter, does not heed the warning set forth by these independent reports, we will put our Nation further

at risk. Much is being done to protect our sensitive information but much more needs to be done.

We began this Congress by holding a hearing into the security concerns at Los Alamos National Lab. We're ending this Congress with yet another hearing into security concerns at the Department of Energy's labs.

All too often we find that security improves at the DOE while Congress, the GAO and the inspector general or the Office of Independent Oversight is shining a light on them. However, far too often labs slip back into their own ways and have yet another security relapse.

The Department can be sure that as long as I am chairman of this subcommittee there will be a constant light shining on them to ensure they are doing all they can to protect our Nation's nuclear materials and secrets.

That is the end of my opening statement. I next turn to Mr. Shimkus, the ranking member, for his opening statement, please.

OPENING STATEMENT OF HON. JOHN SHIMKUS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. SHIMKUS. Thank you, Mr. Chairman. I recognize your valiant effort to fight this cold and turning from a baritone to a bass, it really is Chairman Stupak, and I'll testify to that. But thanks for soldiering on, and thanks for this hearing.

There are few topics the subcommittee will examine as important to our national security as those concerning the security of our national weapons labs. And although I am new to this committee, the Oversight and Investigation Subcommittee has done it for years, and the committee's responsibility has been well noted. And there are few topics where we have been as frustrated as those that concern the security at the labs.

Today's hearing serves as a progress report on work requested by the bipartisan committee and subcommittee leadership. Our requests were prompted by a series of physical and cyber security debacles at Los Alamos National Laboratory and poor performance at Lawrence Livermore National Laboratory in an April 2008 DOE physical security evaluation.

We will hear from the Government Accountability Office this morning on two topics, one concerning physical security and the other one concerning cyber security on the unclassified computer network. The GAO details areas of accomplishment, but also identifies continued significant concerns. Of these concerns, the most troubling involve the cyber threats to what is called the "yellow network," the lab's protected unclassified network. The yellow network serves as a backbone for lab operation and its research mission. However, both the GAO and DOE Independent Office of Health, Safety and Security have identified particular vulnerabilities with the security of the yellow network.

Action is needed to improve the security of the yellow network, but what corrective actions is to take place is based on a risk assessment and risk management. Do DOE and NNSA know or will they know soon exactly what information is on the yellow network? Will DOE and NNSA be willing to identify information that needs

special protection? And will they be able or willing to implement corrective actions?

Are there any recommendations or corrective actions that they believe would be too costly, time consuming or disruptive to implement? If so, what evidence supports that belief? And does it outweigh the cost to national security? Striking that balance is a challenging task.

There are about 13,000 users of the network at Los Alamos, including cleared foreign nationals, some from sensitive nations of concern for security officials. We will hear this morning that the network fire walls deflect more than 10 million cyber probes every month and that threats to cyber defenses are rapidly escalating in number, sophistication and complexity.

And what is the information on this network? It is not classified, but it is sensitive and can have an impact on national security. Panelists will detail some of the categories for us which, GAO reports, presents a valuable target for foreign governments, terrorists and industrial spies.

How robust is network security especially when probed by the most sophisticated adversaries? Have any of the probes succeeded? And if they have, what has been lost? What may be lost? These critical questions underscore the findings of GAO that more needs to be done to protect the network. And if we cannot be satisfied that network protections can safeguard fully the information of these ever-more sophisticated attacks and soon, what other options can we pursue for information security? The answer to this will not be easy, and it involves striking the balance between mission and security, but we have to find an answer.

This GAO testimony provides just the starting point for the security issues we will discuss this morning. When coupled with the government audits and evaluations, the testimony raises important questions that apply not only to the overall security posture at Los Alamos, but at Lawrence Livermore National Laboratory and Sandia National Laboratories as well as labs overseen in Washington.

I look forward to hearing the perspective of the lab directors with us on the second panel, as well as from DOE and the National Nuclear Security Administration officials also on the second panel. I will want to hear their answers to the questions I pose about enhancing the security of the yellow network.

We should identify measures and indicators for progress on improving security going forward as rapidly as possible. We also have to ensure that any measures for security can be sustained for the long term with sufficient flexibility to respond to emerging threats.

And finally we have to recognize the human factor at work here; this means the researchers, the security people and the management. I understand there appear to be two cultures at the lab with different priorities, the research academic culture and the security culture. These solutions need to reflect that reality as well as reconcile the differences.

Thank you, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Shimkus.

Mr. Green for an opening statement, please.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman. And I'll make my statement relatively brief.

I hate to sound like a broken record over these last few years, but it's the subcommittee's 14th hearing on security issues facing the Department of Energy's national labs. I hope that today we can finally show some progress towards securing the critical infrastructure and information of our weapons labs. With the emerging threats facing our Nation, we cannot afford more empty promises of change.

Los Alamos, Livermore and Sandia house America's most sensitive and top secret weapons development programs. The only thing not secret about these labs is that there are security vulnerabilities.

In September 2006, the subcommittee learned how simple it was for a contract employee to remove a USB ThumbDrive containing hundreds of pages of classified documents. Just this year, after a mock terrorist attack by DOE at Livermore, we learned how easily lab security could be compromised through their ill-trained workforce and protective strategy.

Sometimes I think we have to say enough is enough. I do not want to sit through future congressional hearings where we must piece together how a perpetrator gained access to classified nuclear weapons design information from our labs because we did not have the resolve to correct the lab security deficiencies today.

The testimony from this morning's hearing will show that some progress has been made. For example, Los Alamos National Lab has drastically reduced the number of removable electronic media and eliminated thousands of classified nuclear weapons parts and reduced the number of bulk-type rooms and areas containing special nuclear material. These efforts should be commended. But when we are protecting information critical to the national security of the United States, incremental action is notable but not sufficient.

We in Congress owe it to the American people to ensure that weapons labs are safe and secure. And if the Department of Energy or their labs are not up to the task of providing the highest level of protection, Congress must be willing to make the tough choices to protect our national interests.

And again I thank you, Mr. Chairman, for continuing these hearings. I look forward to the testimony, and I yield back my time.

Mr. STUPAK. Thanks, Mr. Green.

Mr. STUPAK. Ms. Blackburn for an opening statement, please.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Ms. BLACKBURN. Thank you, Mr. Chairman. As has been stated, we have had several hearings on the issue of problems with the national labs, and with the accountability or the lack thereof with the labs. It is frustrating to us to see a reticence to make any changes. And I think it is also frustrating to our constituents because now more than ever they are paying close attention to energy issues, to

how the Department of Energy is working, to security issues or lack thereof of security.

And I think that today, as you come before us and as we hold this hearing, and as we are in the midst of this financial crisis, many people are very concerned about a proposed plan to give the Secretary of the Treasury a blank check to bail out Wall Street. And what we're hearing is, they don't trust government. And we know that that lack of trust is going to, therefore, be reflected onto each and every department and agency of the Federal Government. And I think that it amplifies some of the lack of accountability and the hesitancy that we have seen from some of our government agencies and from you.

And the problems with these labs are more—they're just more symptoms of what many people believe to be an incompetence of the bureaucracy in the Federal Government, that you have gotten too big and too unwieldy and too out of control for your own good and definitely for the taxpayers' good.

If these government-run labs cannot protect classified and sensitive information and material, then Congress must begin to discuss alternatives to the current operating procedures that will solve the problems. It would be interesting to know what your best practices are and what your timeline is for meeting those best practices.

Mr. Chairman, I think that protecting that classified material and that sensitive data is one of the key responsibilities of government. And if it does not, then our Nation faces serious risk in the area of breaches of security.

Congress should put forward initiatives. We are going to take the lead on this. If you cannot and will not, then we will. We'll take the lead that will increase transparency, that will demand accountability on behalf of the taxpayers that are footing the bill for this.

And it's not only for you. It is for the entire Federal Government. So as my grandmother would have said, You are on my last nerve; and I hope that you're going to be willing to work with us and increase some accountability and some transparency.

And Mr. Chairman, I will yield back the balance of my time.

Mr. STUPAK. I thank the gentlewoman.

Mr. Dingell, chairman of the full committee, for an opening statement, please.

OPENING STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. DINGELL. Mr. Chairman, good morning. And thank you for your vigorous leadership in the matters before us. And I want to thank you also for holding another important hearing on the distressing state of security at our Nation's weapons labs.

This will be the 14th hearing we've held on this topic over the last 8 years. It was the topic of our first oversight hearing in the 110th Congress and today it may well be one of the last of this Congress.

I feel a little bit like Sisyphus or like Heracles when he was confronted with the Augean Stables. We have before us an agency which has been totally incapable of addressing problems.

Back in the days when I was chairman of the Subcommittee on Oversight and Investigations 20-some years ago, we had hearings. We found a huge problem with regard to security at our Nation's labs. We found that they turned off the sprinkler systems because they didn't want to wet their computer systems. We found they had vehicles, emergency vehicles, that would not start.

We found them with employees in charge of security who did not have the ability physically to participate in the suppression of penetration of those facilities. We found that the tests and the efforts to assure that the Agency could respond to security challenges were carefully cooked by informing the people beforehand what was going to happen so that the drill could take place in the most favorable of circumstances. And we found, curious enough, they still were not able to do the job that had to be done.

We found that there were stings with regard to controlled substances which were suppressed. We found dissipation of public resources and scientific equipment amounting to millions of dollars. We found losses of equipment. And we found inability to keep track of government property.

We found the Agency had to go lightly on their drills because employees charged with security were having heart attacks as a result of having to defend these facilities. It was a situation worthy of the Grand Duchy of Graustark. And it was indeed a situation which would have been humorous were it not for the fact that it was so sad and so dangerous.

I will not burden my colleagues with further details of the events that this committee has had the distressful experience of disclosing over the years. But classified information has disappeared. Drug users have obtained clearances. Sensitive information is being uncovered in drug raids. And promises are made and continually broken to improve security by every administration that has been before this committee.

After our last hearing this hearing asked the Government Accountability Office to conduct a comprehensive review of ongoing security issues at Los Alamos National Lab. Today we're going to hear the results of that work as a result, as well as the results of a number of audits and studies by the Department of Energy's inspector general and its Office of Independent Oversight.

These conclusions are mixed, and I must say that I achieve a small measure of comfort by finding that they're mixed. And at least they are not, for a change, all bad. While GAO found a number of ongoing concerns at Los Alamos National Laboratory that deserved the attention of the committee, they also found some evidence of improvement for which we rejoice, enough to make me slightly optimistic that the lab's security is in some way improving.

This improvement must be tempered, however, by GAO's warning that security at DOE labs appears to be cyclical. I'm not quite sure what that means, but it may relate to the fact that from time to time this committee has hearings to find out how the matter progresses. Indeed, however, it is not clear to me or, I suspect, anybody else how Los Alamos intends to ensure that these problems will not reoccur.

Unfortunately, we will also learn today that while Los Alamos has improved security, another critically important DOE weapons

lab, Lawrence Livermore National Laboratory, has not. In April of 2008, DOE's Office of Independent Oversight completed an evaluation review of security at Livermore. The results, quite frankly, were shocking and sufficiently serious that we can only discuss the specific details in our closed session this afternoon.

I'd like to observe that we have before us identified major problems with key aspects of Livermore's protective strategy, including malfunctioning equipment, inadequate staffing, insufficient training of the protective workforce. And while we understand that many of these shortcomings are being addressed, or at least we're so informed, the OIO findings are so troubling that we must learn more about how DOE allowed this to happen and what they're doing to prevent a recurrence.

Lastly, today, we will hear from an even bigger problem facing these labs and DOE as a whole. And that is the threat from cyber attacks, a new and increasingly serious danger. At our request, GAO conducted a comprehensive review of Los Alamos's unclassified cyber network; and the results of the review highlight the need for significant security improvements to protect sensitive information on Los Alamos's unclassified network.

As noted by the GAO, the information on this network presents a valuable target for foreign governments, terrorists and industrial spies. And it's an interesting thing that this kind of threat enables people to do the kind of penetration of our national security simply sitting in their living room, working with their computers.

This problem, however, is not unique to Los Alamos. All of DOE's labs are facing cyber security challenges. We're going to hear testimony that the labs are virtually naked to concerted cyber attacks, especially by assault from persistent or funded and dedicated assailants right in there, terrorists or foreign governments.

Given the sensitivity of these facilities and the people who work there, we need to learn how DOE is working to correct this problem and when we may expect that it will, in fact, be corrected.

Mr. Chairman, under your leadership I know that this committee is going to continue its examination into cyber security in the next Congress and to broaden it to include all departments and agencies within our jurisdiction. Because the potential consequences of this situation are very, very serious, I expect that this will be one of our most important oversight priorities next year.

And I want to thank you for the work and the leadership that you have done and shown, and express my hope that I will be able to work with you again on this very important matter. Thank you, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Dingell.

[The prepared statement of Mr. Dingell follows:]

PREPARED STATEMENT OF HON. JOHN D. DINGELL

Mr. Chairman, thank you once again for holding another important hearing on the state of security at our Nation's weapons labs. This will be the fourteenth hearing we have held on this subject over the last eight years. It was the topic of our first oversight hearing for the 110th Congress, and today it may conclude this Subcommittee's hearings for this Congress.

I will not bore my colleagues with all the gory details of security misadventure and mishap that this Committee has uncovered over those 8 years-of classified information disappearing, of drug users obtaining clearances, of sensitive information

being uncovered in drug raids, and of promises made and continually broken to improve security.

Rather, after our last hearing, this Committee asked the Government Accountability Office (GAO) to conduct a comprehensive review of ongoing security issues at Los Alamos National Lab. Today we will hear the results of that work as well as the results of a number of audits and studies by the Department of Energy's Inspector General and its Office of Independent Oversight.

Their conclusions are mixed. While GAO found a number of ongoing concerns at Los Alamos National Laboratory that deserve our attention, they also found evidence of some improvement-enough to make me cautiously optimistic that lab security is in some ways improving. However, this improvement must be tempered by GAO's warning that security at DOE labs appears cyclical, and it is not clear how Los Alamos intends to ensure these problems will not reoccur.

Unfortunately, we will also learn today that while Los Alamos has improved security at another critically important DOE weapons lab—Lawrence Livermore National Laboratory—has not.

In April 2008, DOE's Office of Independent Oversight (OIO) completed an evaluation and review of Livermore's security posture. The results were shocking and so serious that we can only discuss the specific details in our closed session this afternoon.

Let me just say that they identified major problems with key aspects of Livermore's protective strategy, including malfunctioning equipment, inadequate staffing, and insufficient training of its protective workforce. While we understand that many of these shortcomings are being addressed, the OIO findings are troubling, and we must learn how DOE allowed this to happen and what they are doing to prevent a reoccurrence.

Lastly, today we will hear of an even bigger problem facing these labs, and DOE as a whole, and that is the threat from cyber attacks. At our request, GAO conducted a comprehensive review of Los Alamos' unclassified cyber network, and the results of this review highlight the need for significant security improvements to protect sensitive information on Los Alamos' unclassified network. As noted by GAO, the information on this network presents "a valuable target for foreign governments, terrorists, and industrial spies."

Unfortunately, this problem is not unique to Los Alamos. All of the DOE labs are facing cyber-security challenges. We will hear testimony that the labs are virtually naked to concerted cyber attacks-especially by assault from persistent, well-funded, and dedicated assailants. Given the sensitivity of these facilities and the people who work there, we need to learn how DOE is going to correct this problem.

I would urge this Subcommittee to continue its examination into cyber security in the next Congress and broaden it to include all departments and agencies within our jurisdiction. I expect this may be one of our most important oversight priorities next year and look forward to working with you on this matter.

Mr. STUPAK. Mr. Burgess for an opening statement, please.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. Thank you, Mr. Chairman. This does seem like deja vu all over again, doesn't it?

We've had hearings in the past and we've established some serious lapses in security and managerial oversight at Los Alamos National Laboratory. Indeed, we went through an entire process with those Requests for Proposals as to whether or not the management of the lab should change.

I took a trip out to Los Alamos in July of 2005. I just wanted to see for myself on the ground. I have got to say, I was impressed by the work being done; I was impressed by the dedication of the employees. But as we continued to hear after that, even after the evaluation and even though there was no management change, but there was promise of some changes, we still heard the reports of things that weren't quite right.

Through all of those hearings, we always heard that things at Sandia, things at Lawrence Livermore were the gold standard, and that's what we should aspire to. But now we have got a GAO report that say significant problems exist in physical and electronic security at Lawrence Livermore as well. So the security of these agencies may have made some progress in strengthening some of the security weaknesses at Los Alamos—and I think that's still in question.

The NNSA needs to be more consistent with their progress in other facilities. Gaps in the physical protection of classified documents, but especially the electronic uses of both classified and unclassified, but sensitive; this committee should maintain persistent oversight until these problems are corrected.

I am concerned with the cyber security weaknesses and lab policies towards the physical protection of computers, portable storage devices and other sensitive areas in the labs. It seems like we've been through this before at Los Alamos, and I guess I have to wonder why we're not learning the lessons as they're given to us.

It's taken for granted that almost any enterprise undertaken in life will involve a computer, a cell phone, a BlackBerry or some other electronic device. It's also a near certitude that an ill-meaning person or persons can attempt to illegally access electronic systems and devices for a variety of reasons, none of which are good. The rapid advancements in technology make the nature of the threat to our electronic systems one that is constantly evolving, therefore we need to be flexible on the committee, but we need to be vigilant.

In 2002, Congress passed the Federal Information Security Management Act to protect our critical information infrastructure. This was before I was elected. And I do wonder if our Federal agencies, particularly the Department of Energy, are in compliance with this important law. It's a dangerous time. Our national security secrets should be closely held, closely guarded; and they should stay our national secrets.

The Office of Inspector General has noted that our nuclear labs and Department of Energy work information systems are compromised. I will look forward to working with the chairman of this subcommittee and the chairman of the full committee to ensure that our nuclear secrets do not fall into the wrong hands.

And I will yield back the balance of my time.

Mr. STUPAK. I thank the gentleman. We have our first panel before us. Let me introduce them if I may:

Mr. Gregory Wilshusen, who is the Director of Information Security Issues at the U.S. Government Accountability Office. And you're accompanied by Ms. Allison Bowden of the GAO. And you are senior auditor, correct? OK. Mr. Glenn Podonsky, who is the Chief Health, Safety and Security Officer in the Office of Health Safety and Security of the Department of Energy; and the Honorable Gregory Friedman, who is the Inspector General at the Department of Energy.

Welcome to all of our witnesses.

It's the policy of this committee to take all testimony under oath. Please be advised you have a right by the Rules of the House to

be advised by counsel during your testimony. Do any of you wish to be advised by counsel during your testimony?

Everybody indicating "no." Therefore, I will ask you to stand, raise your right hand and take the oath.

[Witnesses sworn.]

Mr. STUPAK. Let the record reflect that the witnesses have answered in the affirmative to the oath. They are now under oath.

Mr. STUPAK. We will begin with opening statements.

Mr. Friedman, let's start with you. If you don't mind, pull that mic up. And you are recognized for 5 minutes. If you have a longer statement, it will be submitted for the record. So if you would begin, please.

STATEMENT OF GREGORY H. FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY

Mr. FRIEDMAN. Thank you, Mr. Chairman and members of the subcommittee. I'm pleased to be here today at your request to testify on matters relating to security at the Department of Energy's national defense laboratories. These laboratories, which are part of the National Nuclear Security Administration, process some of the Department's most sensitive information, information which is critical to the Nation's defense.

Since 2002, the Office of Inspector General has categorized information security as one of the Department's most significant management challenges. In April of 2007, I testified before this subcommittee on the special inquiry conducted by my office regarding a diversion of classified data from the Los Alamos National Laboratory, an event made possible in large part by cyber security-related weaknesses.

The Office of Inspector General has continued its efforts in this area by conducting a number of cyber security reviews throughout the Department, including NNSA and its national defense laboratories. Early this year we conducted an extensive review of the process to certify and accredit classified national security information systems. Simply stated, certification and accreditation is a critical management tool used to recognize and address risks by ensuring that cyber security controls are in place.

Our findings relative to the NNSA and its laboratories revealed a number of weaknesses. In particular, we found, first, critical security functions had not been adequately segregated, providing the opportunity for systems security officers to gain access and modify systems without review or approval.

Secondly, risks associated with classified and unclassified systems operating in the same environment had not always been adequately evaluated.

Third, the system security plans omitted information on hardware such as servers, network printers, and scanners, a condition paralleling one of our concerns relating to the diversion of classified material at Los Alamos.

And finally, contingency plans outlining actions necessary to resume operations in the event of a disaster were not always developed or they were incomplete.

These weaknesses occurred, in part, because the NNSA had not been fully successful in ensuring its laboratories implemented the

Department's updated cyber security requirements. For example, two laboratories completed their certification and accreditation process using outdated requirements, leaving a number of systems vulnerable to control weaknesses. In addition, headquarters and field site officials had not effectively reviewed security plans to ensure that they were accurate and adequately addressed system risks.

In our recently issued Federal Information Security Management Act evaluation, we identified a number of weaknesses that exposed unclassified systems to an increased risk of compromise.

We found, first, two of the three defense labs had not yet completed certification accreditation of certain business systems, a deficiency first reported in 2006.

Mandatory security controls were not included in systems security plans at one laboratory.

All three laboratories had not completed implementation of the federally mandated standard desktop configuration.

Computer incident reports did not always include information needed for implementing—needed for reporting to law enforcement and for subsequent analysis for trending.

And at one laboratory vulnerabilities were identified that may have allowed unsupervised foreign visitors to inappropriately access the site's intranet.

We found that NNSA had not in a timely manner incorporated Federal and departmental cyber security requirements into its policies and guidance. In addition, NNSA also had not effectively completed reviews and performance monitoring, activities essential for evaluating the adequacy of cyber security operations.

Our evaluations reveal a mixed picture. The Department and NNSA have improved their cyber security efforts, yet weaknesses still exist. Additional action is necessary to protect systems and the information they contain from increasingly sophisticated and persistent attacks.

Since the end of fiscal year 2007, as has been referred to earlier in the opening statements, the Department has experienced a 45 percent increase in reported cyber security incidents. This significant increase demonstrates the need for sustained action in securing the Department's information systems.

Our work suggests that there are some recurring challenges that NNSA should consider as it moves forward. Specifically, NNSA should implement in a timely manner all relevant Federal departmental cyber security requirements, strengthen the management and review process by better monitoring field sites to ensure adequacy of cyber security program performance and, finally, ensure that all outstanding cyber security weaknesses are corrected in a timely manner.

The Office of Inspector General recognizes well the importance of cyber and physical security and we are committed to continuing our work in these areas.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions you may have.

Mr. STUPAK. Thank you Mr. Friedman.

[The prepared statement of Mr. Friedman follows:]

STATEMENT OF GREGORY H. FRIEDMAN

SUMMARY

• Since 2002, the Office of Inspector General (OIG) has categorized information security as one of the Department of Energy's (Department) most significant management challenges. While incremental improvements have been made to improve security and reduce risks to systems and data, additional work needs to be done.

• The OIG recently issued a report on the certification and accreditation of the Department's national security information systems. Our review disclosed that weaknesses exist in the areas of risk management, security planning, and contingency planning. In addition, the National Nuclear Security Administration (NNSA) had not been fully successful in ensuring that its laboratories implemented the Department's updated, strengthened policies designed to protect national security information systems.

• A Fiscal Year 2008 review of the Department's unclassified cyber security program identified opportunities for improvements in areas such as certification and accreditation of systems, systems inventory, contingency planning and segregation of duties.

• The problems identified occurred because NNSA had not revised and implemented, in a timely manner, policies and guidance incorporating Federal and Departmental cyber security requirements. NNSA also had not effectively completed review and performance monitoring activities essential for evaluating the adequacy of cyber security operations.

• Since the end of Fiscal Year 2007, the Department has experienced a 45 percent increase in reported cyber security incidents. This significant increase demonstrates the need for sustained action in securing the Department's information systems.

STATEMENT

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on matters relating to cyber security at the Department of Energy's (Department) national defense laboratories. These laboratories, which are part of the National Nuclear Security Administration (NNSA), possess and process some of the Department's most sensitive information; information which is critical to the Nation's defense.

BACKGROUND

The Office of Inspector General (OIG) has a long-standing, proactive program to assess the effectiveness of the Department of Energy's cyber security strategy. Since 2002, the OIG has categorized information security as one of the Department's most significant management challenges. In April of 2007, I testified before this Subcommittee on the special inquiry conducted by my office regarding a diversion of classified data from the Los Alamos National Laboratory; an event made possible, in large part, by cyber security related weaknesses. The OIG has continued its efforts in this area by conducting a number of cyber security reviews throughout the Department, including NNSA and its national defense laboratories - Los Alamos, Lawrence Livermore, and Sandia.

REVIEW OF NATIONAL SECURITY INFORMATION SYSTEMS

In response to our special inquiry on the diversion of classified data at Los Alamos, the Department initiated a wide range of actions to address cyber security weaknesses related to classified systems. For instance, the Department updated and strengthened its national security information systems policy for segregation of duties and system access techniques.

Earlier this year, we conducted an extensive review of the process to certify and accredit classified national security information systems at the NNSA laboratories. Certification and accreditation (C&A) is a critical part of the risk management process and is vital to understanding and mitigating cyber-related vulnerabilities. This process is designed to ensure that systems are secure prior to beginning operation and that they remain so throughout their lifecycle. It includes formal steps to: (1) recognize and address risks, (2) determine whether system security controls are in place and operating effectively, and (3) ensure that changes to systems are adequately tested and approved. Our findings relevant to the NNSA and its national defense laboratories revealed that:

• Critical security functions had not been adequately segregated, providing the opportunity for system security officers to gain access and modify systems without review or approval, creating an environment in which controls could be manually overridden;

• Risks associated with classified and unclassified systems operating in the same environment had not always been adequately evaluated. This weakness - exacerbated by the lack of segregation of duties - increased the risk that classified information could be transferred to unclassified systems;

• Users at one laboratory were allowed to manually change passwords, a practice specifically prohibited by the Department and one which rendered passwords on classified systems more susceptible to compromise;

• At the same laboratory, a number of security plans were not reviewed and approved by a Federal official, depriving NNSA of the opportunity to ensure that all risks to the systems were addressed;

• System security plans omitted information on hardware such as servers, network printers and scanners, the presence of which could have created a security vulnerability and enabled the unauthorized processing, diversion or theft of classified material. This condition paralleled one of our concerns related to the diversion of classified information at Los Alamos; and,

• Contingency plans outlining actions necessary to resume operations in the event of a disaster were not always developed or were incomplete.

The Department had strengthened policies designed to protect national security information systems in response to our recommendations following the Los Alamos incident. However, NNSA had not been fully successful in ensuring that its laboratories implemented these updated and stronger requirements. For example, two laboratories completed their C&A process using outdated requirements, leaving a number of systems vulnerable to control weaknesses such as the lack of segregation of duties and strong authentication techniques. In addition, Headquarters and field site officials had not effectively reviewed security plans to ensure that they were accurate and that they adequately addressed system risks.

REVIEW OF UNCLASSIFIED SYSTEMS

The OIG has also devoted substantial resources to evaluating security measures designed to protect the Department's unclassified information systems and data. The Federal Information Security Management Act requires that agency Inspectors General conduct an annual independent evaluation of their Department's unclassified cyber security program and practices. Our recently issued Fiscal Year (FY) 2008 evaluation revealed a mixed-picture: on one hand, the Department had made incremental improvements in its unclassified cyber security program. For example, various sites had taken action to address weaknesses we identified during our FY 2007 evaluation by strengthening configuration management, updating policy, and incorporating cyber security performance requirements into management and operating contracts. However, a number of weaknesses that exposed systems to an increased risk of compromise still existed within the Department. This specifically included NNSA and its national defense laboratories. In particular:

• Two of the three defense laboratories had not yet completed certification and accreditation of certain business systems, a deficiency we first reported in FY 2006;

• System security plans at one laboratory did not include mandatory security controls. Such information is necessary for management to determine that all system risks have been fully considered and that mitigating controls are in place;

• At one laboratory, unneeded computer services had not been disabled on over 40 servers that hosted publicly accessible websites. These services, which in a number of instances could be accessed without the use of passwords or other authentication techniques, increased the risk of malicious damage to the servers and the networks on which they operated;

• All three laboratories had not yet completed the deployment of the Federally-mandated standard desktop configuration, an action that when implemented is intended to significantly enhance cyber-related controls;

• Computer incident reports did not always include information needed for reporting to law enforcement and for subsequent analysis for trending. Further, reported information was not always shared with other Department elements; and,

• At one laboratory, vulnerabilities were identified that may have allowed unsupervised foreign visitors to inappropriately access the site's intranet. Such practices, if exploited, could have permitted those individuals to probe the laboratory's network for vulnerabilities, implant malicious code, or remove data without authorization.

ISSUES REQUIRING CONTINUING ATTENTION

While NNSA has taken steps to address a number of weaknesses identified in the past, additional action is necessary to protect systems and the information they contain from increasingly sophisticated and persistent attacks. Since the end of FY 2007, the Department has experienced a 45 percent increase in reported cyber security incidents. This significant increase demonstrates the need for sustained action in securing the Department's information systems.

Our work suggests that there are some recurring challenges that NNSA should consider as it moves forward. Specifically, NNSA should:

1. Implement, in a timely manner, all relevant Federal and Departmental cyber security requirements;
2. Strengthen the management review process by better monitoring field sites to ensure the adequacy of cyber security program performance; and,
3. Ensure that all outstanding cyber security weaknesses are corrected in a timely manner.

To achieve the recommended reforms as promptly as possible, NNSA should establish firm schedules with specific implementation timeframes and benchmarks.

ONGOING INSPECTOR GENERAL EFFORTS

Both cyber and physical security continue to be pressing management challenges. For that reason, the Office of Inspector General has ongoing activities to examine information technology and systems security, implementation of physical security technology upgrades, protection of sensitive unclassified information, and accounting for nuclear materials in the hands of domestic licensees.

Mr. Chairman, this concludes my statement and I would be pleased to answer any questions you may have.

Mr. STUPAK. Mr. Podonsky, please, for your opening statement.

STATEMENT OF GLENN S. PODONSKY, CHIEF HEALTH, SAFETY AND SECURITY OFFICER, U.S. DEPARTMENT OF ENERGY

Mr. PODONSKY. Chairman Stupak, Ranking Member Shimkus and members of the subcommittee, I want to thank you for inviting me to testify today on the status of the security and cyber security programs at the Department of Energy's three weapons laboratories.

As the Department's Chief Health, Safety and Security Officer, my office and I have a direct interest in the levels of rigor and effectiveness at which these laboratories and all DOE sites implement the Department's security requirements.

In the area of physical protection and the protection of special nuclear material, the HSS Office of Independent Oversight conducted a comprehensive security inspection this past spring at Lawrence Livermore National Laboratory and just recently completed an inspection at Los Alamos National Laboratory. While there were a number of identified weaknesses, most notably at Lawrence Livermore, reports of progress indicate that they are aggressively addressing identified deficiencies. We will validate the effectiveness of these corrective actions when we conduct a follow-up inspection in the spring.

The results of our evaluations indicate that the systems in place to protect classified matter at these laboratories are generally adequate and in compliance with expectations, but there are residual issues that must be addressed. In the area of cyber security, threats to DOE and NNSA cyber security defenses continue to escalate both in terms of the number of attacks and in the sophistication and complexity of those attacks.

Mr. Chairman, DOE, along with many other government agencies and corporate organizations, are experiencing a broad range of cyber security threats that we must protect against on a continuous basis. Our interconnected society and dependency on the rapid exchange of vast quantities of electronic information exposes all of us to cyber threats similar to those faced by DOE and NNSA. I believe the entire U.S. Government is at a crossroads on how we protect sensitive information.

Our independent oversight inspections have identified numerous positive attributes of the classified cyber security programs at each of the weapons laboratories, and while there are some deficiencies that need to be addressed, the classified cyber security program throughout DOE remains strong.

Unclassified cyber security presents a different challenge. The primary threats to our unclassified networks used to be directed at our perimeter defenses, and as a result, the Department directed significant effort toward strengthening its network perimeter through implementation of fire walls and intrusion detection systems. However, as external network's defenses have grown stronger, our adversaries have shifted strategies and most attacks today are less direct.

Many new network penetrations now occur as a result of an authorized user activating malicious software program commonly used known as a Trojan horse or some form of social engineering. Once a user activates a malicious program, a communication channel is established to the adversary system, essentially ignoring the otherwise effective fire wall.

In January of 2005, my office added to our existing inspection program an unannounced network testing process commonly referred to as "red teaming" to provide a more rigorous evaluation of this new threat environment. Red teaming evaluates the strengths and weaknesses and security controls, as well as the Department's ability to detect and disseminate information about attacks and how it addresses the attacks.

Our most recent red team activity, conducted with only six cyber specialists and in under 90 days, resulted in our ability to take full control of two site networks and one small site office network. Our red team was able to download a very large quantity of data in gigabytes, 40,000 documents, some of which were sensitive without being detected.

Additionally, with this access, we installed our own malicious programs on a number of laptop computers. As these laptops were legitimately connected to other networks through authorized accounts, we were able to see these networks and to browse the information on them, thus demonstrating our ability to migrate through the Department into sensitive networks.

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

sensitive unclassified information to sources outside their networks.

The DOE Chief Information Officer and the Under Secretaries have made progress in recent years with respect to developing new policy and governance model to implement these new policies. This governance model essentially enables each Under Secretary to determine how they will implement departmental requirements through their programmed cyber security plans. Our inspections, however, have continued to demonstrate that some fundamental cyber security requirements are not consistently implemented throughout the Department.

We don't want to underestimate the work that has already taken place. Some sites, especially within NNSA, have addressed many of these issues. However, the Department continues to identify successful penetrations of our networks.

To protect sensitive information more effectively, we need to enhance certain aspects of departmental policy to include requiring encryption of sensitive information stored on all computers, implementing a more robust program cyber security plan and review process by the DOE's Office of the CIO to ensure that the plans are meeting expectations and revisiting some of the risk decisions that have been made with particular emphasis on the evolving threat environment.

Additionally, we need to continue to educate our users regarding the threats involved with opening attachments and running programs from untrusted sources. We should implement authenticated gateways for all outbound Internet access to reduce the ability for automated programs to establish pathways to external systems, as we did with our red team. We should also more efficiently analyze suspicious activities across the network. Finally, we need to do a better job of keeping attackers who manage to gain access to sensitive information on our systems from sending that data outside our network perimeters as well as limit their ability to migrate to other areas of the site's network.

Mr. Chairman, my office and I believe this subcommittee and DOE share the same goal of ensuring that our national security assets are well protected and also share the concern when the protection effectiveness falls below our standards. However, the Department and the laboratories have additional work to do to ensure that protection of the classified information they possess in both physical and electronic form.

I cannot stress strongly enough our belief that we need to get back to the basics of risk management to identify which information needs special protection, to determine appropriate protection measures to apply to that information, and then we need to ensure that the protection measures are actually implemented.

Thank you, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Podonsky.

[The prepared statement of Mr. Podonsky follows:]

TESTIMONY OF
GLENN S. PODONSKY
CHIEF HEALTH, SAFETY AND SECURITY OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

September 25, 2008

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

Office of Health, Safety and Security Responsibilities

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

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

Protection of Special Nuclear Materials

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

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

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

Protection of Classified Matter

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

Cyber Security

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

Classified Cyber Security

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

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

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

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

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

Unclassified Cyber Security

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

Mr. STUPAK. Mr. Wilshusen, your opening statement, please, sir.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES; ACCOMPANIED BY ALLISON BOWDEN, SENIOR AUDITOR, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Stupak, Ranking Member Shimkus and members of the subcommittee.

Mr. STUPAK. Is your mic on, sir? Just pull it up a little bit, if you don't mind.

Mr. WILSHUSEN. Can you hear me now? OK.

Chairman Stupak, Ranking Member Shimkus and members of the subcommittee, I am pleased to be here today to testify on physical and cyber security at the Los Alamos National Laboratory or LANL, one of three national laboratories operated by the National Nuclear Security Administration that designs and develops nuclear weapons for the U.S. stockpile. I am joined by Allison Bowden, a GAO senior analyst specializing in physical security.

A basic management objective for any organization is to protect the assets and resources that support its critical operations from theft, unauthorized access, use, modification, destruction or disruption. It is especially critical for national laboratories, such as LANL, that possess and process special nuclear material, nuclear weapons parts and highly sensitive and classified information.

A successful physical or cyber attack on LANL could have devastating consequences for the site, its surrounding communities and the Nation's security. Because of these risks, LANL needs effective physical and cyber security programs. Today I will summarize our recently completed work on physical and cyber security at Los Alamos and share our preliminary observations on physical security at the Lawrence Livermore National Laboratory.

Mr. Chairman, LANL is improving its physical security. It is implementing over two dozen initiatives to reduce, consolidate and better protect its classified assets. It has reduced the physical footprint of the laboratory by closing unneeded facilities, although this initiative is focused more on reducing maintenance costs than addressing facility security.

Other challenges remain. Significant physical security problems related to nuclear weapon part storage, inadequate self-assessments and complete corrective action plans have been fully addressed—or have not been fully addressed at the time of our review.

In addition, LANL's ability to sustain security improvements over the long term is unproven because its approach is for sustaining progress contained weaknesses in the early stages of development. For example, a system intended to track long-term improvements would not be fully completed for 3 to 4 years.

Furthermore, the Los Alamos site office, which is responsible for overseeing security at LANL, may not have enough staff or the proper training to provide effective security oversight.

To help strengthen LANL's physical security program, GAO recommended, among other things, that LANL develop a comprehensive strategic plan for addressing identified weaknesses and improving program effectiveness.

At Lawrence Livermore our preliminary observations on physical security indicate that its self-assessment and performance-assurance testing programs need improvement and that NNSA and the Livermore site office have not always provided effective security oversight. Both Livermore and the site office have actions under way that are intended to improve these deficiencies. However, similar to LANL, sustaining improvements may be a continuing challenge.

Turning to cyber security—and in reports being released today, Mr. Chairman, we note that Los Alamos has implemented numerous measures to enhance cyber security, but weaknesses remain that impair the laboratory's ability to sufficiently protect the confidentiality, integrity and availability of sensitive information on the unclassified network. At the time of our site visits, LANL had vulnerabilities in several critical areas, including, identifying and authenticating users of the networks, encrypting certain sensitive information, monitoring compliance with security policies, implementing and testing software patches, and planning for contingencies when the network services are disrupted. A key reason for these weaknesses is that the laboratory had not fully implemented its cyber security program to ensure that controls were effectively established and maintained.

In addition, the number of foreign nationals who have access to the unclassified network, including about 300, as of May 2008, from DOE's designated sensitive countries, had raised concerns amongst some laboratory and NNSA officials because of the sensitive information contained on the network.

To enhance cyber security over the unclassified network, we are making a total of 52 recommendations to improve LANL's program activities, correct specific control weaknesses, and ensure a clear and consistent strategy for determining resource requirements based on risk.

In summary, LANL has taken steps to improve its physical and cyber security programs, but more remains to be done. Until known deficiencies are adequately addressed and improvements sustained over the long term, sensitive and classified resources will remain at increased and unnecessary risk.

Mr. Chairman, we'd be happy to answer any questions.

Mr. STUPAK. Thank you.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, September 25, 2008

NUCLEAR SECURITY

Los Alamos National Laboratory Faces Challenges In Sustaining Physical and Cyber Security Improvements

Statement of Gene Aloise, Director
Natural Resources and Environment

Nabajyoti Barkakati, Chief Technologist
Applied Research and Methodology

Gregory C. Wilshusen, Director
Information Security Issues

GAO-08-1180T

September 25, 2008

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-1180T, testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

NUCLEAR SECURITY

Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements

Why GAO Did This Study

Los Alamos National Laboratory (LANL) is one of three National Nuclear Security Administration (NNSA) laboratories that designs and develops nuclear weapons for the U.S. stockpile. LANL employees rely on sensitive and classified information and assets that are protected at different levels, depending on the risks posed if they were lost, stolen, or otherwise compromised. However, LANL has experienced several significant security breaches during the past decade.

This testimony provides GAO's (1) views on physical security at LANL, as discussed in *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (June 13, 2008); (2) preliminary observations on physical security at Lawrence Livermore National Laboratory; and (3) views on cyber security at LANL as discussed in *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Sept. 9, 2008). To conduct this work, GAO analyzed data, reviewed policies and procedures, interviewed laboratory officials, and conducted site visits to the two laboratories.

To view the full product, including the scope and methodology, click on GAO-08-1180T. For more information, contact Gene Aloise at (202) 512-3841, or aloisee@gao.gov; Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov; and Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov.

What GAO Found

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to better protect its classified assets. However, while LANL's current initiatives address many physical security problems previously identified in external security evaluations, other significant security problems have received insufficient attention. In addition, the management approaches that LANL and NNSA intend to use to sustain security improvements over the long term are in the early stages of development or contain weaknesses. Furthermore, LANL's ability to sustain its improved physical security posture is unproven because (1) the laboratory appears not to have done so after a significant security incident in 2004, with another significant security breach in 2006, and (2) NNSA's Los Alamos Site Office—which is responsible for overseeing security at LANL—may not have enough staff or the proper training to execute a fully effective security oversight program. GAO's report made recommendations to help further improve physical security at LANL and ensure that these improvements are sustained over the long term.

As a result of poor performance on an April 2008 physical security evaluation conducted by the Department of Energy's (DOE) Office of Independent Oversight, GAO is reviewing physical security at Lawrence Livermore National Laboratory (Livermore). GAO's preliminary observations are that Livermore appears to experience difficulties similar to LANL's in sustaining security performance. Furthermore, it appears that NNSA has not always provided effective oversight of Livermore. Specifically, an NNSA security survey conducted only 6 months prior to the April 2008 DOE evaluation gave Livermore the highest possible rating on its security program's performance. These results differ markedly from those documented by DOE's Office of Independent Oversight.

LANL has implemented measures to enhance cyber security, but weaknesses remain in protecting information on its unclassified network. This network possesses sensitive information such as unclassified controlled nuclear information, export control information, and personally identifiable information about LANL employees. GAO found vulnerabilities in critical areas, including (1) identifying and authenticating users, (2) encrypting sensitive information, and (3) monitoring and auditing security policy compliance. A key reason for these information security weaknesses is that the laboratory has not fully implemented an information security program to ensure that controls are effectively established and maintained. Furthermore, deficiencies in LANL's policies and procedures raise additional concern, particularly with respect to foreign nationals' accessing the network from the laboratory and remotely. Finally, LANL cyber security officials told GAO that funding to address some of their security concerns with the laboratory's unclassified network has been inadequate. However, NNSA officials asserted that LANL had not adequately justified its requests for additional funds. GAO made 52 recommendations to help strengthen LANL's information security program and controls over the unclassified network.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss physical and cyber security at Los Alamos National Laboratory (LANL). LANL, located in Los Alamos, New Mexico, has a multibillion dollar annual budget and is one of three National Nuclear Security Administration (NNSA) laboratories responsible for designing and developing a safe, secure, and reliable nuclear weapons deterrent.[1] In fiscal year 2007, LANL budgeted nearly $200 million to provide the laboratory with physical and cyber security to protect the sensitive and classified assets on which laboratory employees rely to conduct their work. A successful physical or cyber attack on NNSA sites containing nuclear weapons, the material used in nuclear weapons, or information pertaining to the people who design and maintain the U.S. nuclear deterrent could have devastating consequences for the site, its surrounding communities, and the nation's security. Because of these risks, NNSA sites need effective physical and cyber security programs.

Over the last decade, LANL has experienced a series of high-profile security incidents in which sensitive assets and classified information were compromised. In October 2006, during a drug raid on a private residence, it was discovered that a LANL contract employee had transferred classified information to a USB "thumb drive" and removed the thumb drive, as well as a large number of classified documents, from the laboratory. The Department of Energy's (DOE) Inspector General reported that a serious breakdown in core laboratory physical and cyber security controls contributed to the October 2006 thumb drive incident.[2] More recently, in April 2008, DOE's Office of Independent Oversight conducted an evaluation of security at Lawrence Livermore National Laboratory (Livermore). The evaluation included a mock terrorist attack on a sensitive laboratory facility and concluded that Livermore's security program had significant weaknesses, particularly with respect to the performance of Livermore's protective force and the physical protection of classified resources.

[1]The other design and development laboratories are Lawrence Livermore National Laboratory in Livermore, California, and Sandia National Laboratories in Albuquerque, New Mexico, and Livermore, California. NNSA is a separately organized agency within the Department of Energy that is responsible for the management and security of the nation's nuclear weapons, nuclear nonproliferation, and naval reactors programs.

[2]U.S. Department of Energy, Office of Inspector General Office of Audit Services, *Special Inquiry Report to the Secretary: Selected Controls Over Classified Information at the Los Alamos National Laboratory,* OAS-SR-07-01 (Washington, D.C., Nov. 2006).

As a result of the October 2006 thumb drive incident and the congressional hearings that followed, the Committee asked us to review physical and cyber security at LANL. In addition, in June 2008, this Committee requested that we review the status of physical security at Livermore. Our testimony today discusses (1) physical security at LANL, (2) preliminary observations from ongoing work on physical security at Livermore, and (3) cyber security at LANL. This statement is primarily based on recently issued reports on physical and cyber security at LANL.[3] We conducted the performance audit work that supports this statement in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to produce a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our statements today.

Summary

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to better protect its classified assets. However, while LANL's current initiatives address many security problems previously identified in external evaluations, other significant security problems have received insufficient attention. For example, at the time of our review, LANL had not implemented complete security solutions to address either the storage of classified nuclear weapons parts in unapproved storage containers or weaknesses in its process for ensuring that actions taken to correct security deficiencies are completed. Furthermore, management approaches that LANL and NNSA officials told us they would use to sustain security improvements over the long term were in the early stages of development or contained weaknesses. In addition, LANL's ability to sustain its improved physical security posture is unproven because (1) the laboratory appears not to have done so after a significant security incident in 2004, and (2) NNSA's Los Alamos Site Office—which is responsible for overseeing physical security at LANL on a daily basis—may not have enough staff or the proper training for these staff to execute a fully effective security oversight program. Our report on physical security at LANL made three recommendations to the Secretary of Energy and the Administrator of NNSA concerning long-term strategic security planning and the use of

[3]GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (Washington, D.C.: June 13, 2008) and GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

meaningful financial incentives for effective security performance. We believe these recommendations, if effectively implemented, would help further improve physical security at LANL and ensure that these improvements are sustained over the long term.

Though our observations on physical security at Livermore are preliminary, the laboratory appears to be experiencing difficulties similar to LANL's in sustaining physical security performance. In addition, Livermore's self-assessment and performance assurance programs appear to need improvement. For example, Livermore and NNSA security officials acknowledged that a lack of comprehensive performance assurance testing was a significant contributing factor to the poor performance of Livermore's protective forces during their April 2008 exercise. Finally, it appears that NNSA has not always provided effective security oversight of Livermore. Specifically, a 2007 NNSA security survey gave Livermore the highest possible rating on its security performance, differing markedly from what DOE observed during its evaluation in April 2008, only 6 months later. DOE identified multiple areas for significant improvement, and gave Livermore the lowest rating possible in two security performance areas.

Our review of cyber security at LANL found that the laboratory has implemented measures to enhance its information security, but weaknesses remain in protecting the confidentiality, integrity, and availability of information on its unclassified network.[4] LANL's unclassified network contains sensitive information, such as unclassified controlled nuclear information, export control information, and personally identifiable information about laboratory employees. LANL has implemented a network security system that is capable of detecting potential intrusions; however, we found vulnerabilities in several critical areas, including identifying and authenticating users; encrypting sensitive information; and monitoring and auditing compliance with security policies. For example, LANL has implemented strong authentication measures for accessing its unclassified network, but once access is initially gained, a user can work around the authentication measures to access certain sensitive information. A key reason for LANL's information security weaknesses is that the laboratory has not fully implemented an information security program to ensure that controls are effectively

[4]We are currently reviewing information security controls over LANL's classified network for this Committee.

established and maintained. For example, LANL's most recent risk assessment for its unclassified network generally identified and analyzed vulnerabilities, but did not account for risks identified by the laboratory's own internal vulnerability testing. Furthermore, we and other external security evaluators have reported concerns about LANL's policies for granting foreign nationals—particularly those from countries classified as "sensitive" by DOE—access to the unclassified network. Finally, LANL cyber security officials told us that funding to address some of their security concerns with respect to the laboratory's unclassified network has been inadequate. NNSA officials told us LANL has not adequately justified its request for additional funds, and NNSA is developing a process for developing cyber security budgets more systematically. We made 52 recommendations to the Secretary of Energy and the Administrator of NNSA that, if effectively implemented, would improve LANL's information security program and controls over its unclassified network. These recommendations address, among other things, ensuring that LANL's risk assessment for its unclassified network evaluates all known vulnerabilities and is revised periodically, and strengthening policies with a view toward further reducing, as appropriate, foreign nationals' access to the unclassified network.

Background

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access, use, destruction, or disruption. Organizations accomplish this objective by designing and implementing controls that are intended to, among other things, prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. At LANL, these assets include Category I special nuclear material, such as plutonium and highly enriched uranium;[5] thousands of classified nuclear weapons parts and components; millions of classified documents; thousands of pieces of classified removable electronic media that contain nuclear weapon design information;[6] over 100 vaults and vault-type rooms that store classified assets; and computer networks and the hardware on which these

[5]Special nuclear material is considered to be Category I when it is weapons-grade, such as plutonium and highly enriched uranium, and occurs in specified forms and quantities.

[6]Some classified documents and pieces of removable electronic media, such as CDs and thumb drives, pose a security risk that requires maintenance of an accountability system to prevent unauthorized access or removal.

networks run that protect classified information as well as sensitive unclassified information.

LANL is subject to a series of DOE security orders that outline requirements for implementing effective physical and cyber security protection strategies. These orders include an assessment of the potential size and capabilities of terrorist forces that could physically attack a laboratory and against which a laboratory must be prepared to defend. The orders further describe different levels of physical protection for sensitive and classified assets, depending on the risk they would pose if they were lost, stolen, or otherwise compromised. Appropriate physical protection safeguards include locks and keys, fences, means to detect unauthorized entry, perimeter alarms, vehicle barriers, and armed guards.

In addition, the Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and information systems across the federal government.[7] FISMA requires each agency to develop, document, and implement an agencywide information security program that supports the operations and assets of the agency, including those provided or managed by another agency or contractor on its behalf. Examples of appropriate information security controls include user identification and authentication that allow computer systems to differentiate between users and verify their identities; cryptography that ensures the confidentiality and integrity of critical and sensitive information; configuration management that identifies and manages security features for all hardware, software, and firmware components of an information system and controls changes to them; and audit and monitoring controls that help establish individual accountability and monitor compliance with security policies.

LANL is managed and operated by a corporate entity, Los Alamos National Security LLC (LANS).[8] NNSA's Los Alamos Site Office serves as the primary federal overseer of laboratory security performance. Annually, the Site Office determines how much money LANS will earn for its

[7]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

[8]LANS has been the management and operating contractor of LANL since June 2006. LANS is made up of the University of California, Bechtel National, Washington Group International, and BWX Technologies (which now operates under the name The Babcock & Wilcox Company).

management of the laboratory according to a maximum available performance-based fee established in the laboratory's contract. The Site Office bases its determination on the laboratory's success in meeting the goals laid out in performance evaluation plans. These plans allocate portions of the maximum available performance award fee to NNSA performance objectives, including measures related to both physical and cyber security.

In addition, two DOE organizations are required to periodically review physical and cyber security at LANL. NNSA's Los Alamos Site Office is required to conduct security surveys annually. These surveys are based on observations of performance, including compliance with DOE and NNSA security directives. In fiscal year 2008, the results of this survey are directly tied to NNSA's performance evaluation plan, and are therefore a factor in LANS' ability to earn the maximum available performance award fee. DOE's Office of Independent Oversight also conducts evaluations, typically every 18 months for facilities that store Category I special nuclear material. These evaluations identify weaknesses in the laboratories' security programs and produce findings that laboratory officials must take action to correct. The reviews overlap substantially, but each is required to provide a comprehensive assessment of the laboratory's security programs.

While Physical Security at Los Alamos National Laboratory Has Improved, Management Approaches to Sustain Security Improvements Are in the Early Stages of Development or Contain Weaknesses

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to reduce, consolidate, and better protect its classified assets, as well as reduce the physical footprint of the laboratory by closing unneeded facilities. LANL officials believe that these initiatives will reduce the risk of incidents that can result in the loss of control over classified assets. For example, to reduce and consolidate classified assets and its physical footprint, as of March 2008, LANL had (1) reduced from nine to one the number of areas containing Category I special nuclear material; (2) reduced the amount of accountable classified removable electronic media from 87,000 pieces to about 4,300 and made information previously accessible on removable media available only through the laboratory's classified computer network; (3) eliminated about 30,000 classified nuclear weapon parts; and (4) reduced the number of vault-type rooms from 142 to 111. In addition, during fiscal year 2007, LANL reduced the physical footprint of existing facilities by over 500,000 square feet. In concert with these actions, LANL is implementing a series of engineered and administrative controls to better protect and control classified assets, [9] such as removing the functions from classified computers that enable them to create new pieces of removable electronic media and streamlining physical security procedures to make them easier to implement across the laboratory.

We found that DOE's Office of Independent Oversight and the Los Alamos Site Office identified significant physical security problems at LANL that the laboratory had not fully addressed. Specifically, while LANL's storage of classified parts in unapproved storage containers and its process for ensuring that actions to correct identified security deficiencies have been cited in external security evaluations for years, complete security solutions in these areas had not yet been implemented at the time of our review. In addition, external security evaluations had repeatedly identified concerns about the adequacy of LANL's assessments of its own security performance. The security self-assessment program provides LANL with the opportunity to self-identify security deficiencies and address them before they can be exploited. External security evaluations found that LANL's self-assessments were not comprehensive and did not include discussions of all internal findings. These evaluations also noted that findings identified through self-assessments were not always analyzed and

[9] Engineered controls are system-based controls that manage work processes and prevent employees from taking inappropriate action. Administrative controls are typically policies or procedures that govern the handling of classified resources.

addressed through corrective actions. At the time of our review, Los Alamos Site Office and DOE Office of Independent Oversight officials noted that LANL's self-assessment program was improving.

LANL officials identified three management approaches that they asserted would sustain security improvements over the long term. However, these approaches were either in an early stage of development or contained important weaknesses that may impair their ability to ensure the sustainability of security improvements at the laboratory for the foreseeable future. First, LANL officials identified completing the management actions required by the Secretary of Energy's Compliance Order issued as a result of the October 2006 thumb drive incident as an approach to ensure that security improvements are sustained, yet the Compliance Order itself does not provide a mechanism to sustain security improvements over the long-term.[10] Second, LANL officials told us they will track the implementation of longer-term actions, including those required by the Compliance Order, by developing and implementing the Contractor Assurance System required under the LANS contract.[11] However, the extent to which LANL can rely on the Contractor Assurance System to ensure the long-term sustainability of security improvements is unclear. According to a Los Alamos Site Office official, the Contractor Assurance System will not be fully completed for 3 to 4 years and, thus, will not be fully implemented by the time actions under the Compliance Order are completed. Finally, according to LANL officials, the laboratory plans to realize security improvements by meeting the security-related performance incentives in the annual performance evaluation plans NNSA uses to measure performance and determine an award fee for LANS. However, the annual performance evaluation plans focus principally on

[10]The Secretary of Energy has authority under 10 C.F.R. § 824.4(b) of DOE's *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations* to issue compliance orders that direct management and operating contractors to take specific corrective actions to remediate deficiencies that contributed to security violations. On July 12, 2007, the Secretary of Energy issued a compliance order to LANS as a result of the security incident discovered in October 2006. The Compliance Order directs LANS to take comprehensive steps to ensure that it identifies and addresses critical classified information and cyber security deficiencies at LANL. Violation of the Compliance Order would subject LANS to civil penalties of up to $100,000 per violation per day until compliance is reached.

[11]The Contractor Assurance System is intended to be a tool to increase accountability and improve laboratory management and performance. According to a LANL official, the Contractor Assurance System is an integrated performance-based management system that is available as a tool for federal oversight.

compliance with DOE requirements and do not sufficiently reward security program improvement. In that regard, according to a senior NNSA security official, compliance with current DOE requirements does not assure that LANL's security program is functioning effectively. Indeed, we found that all but $30,000 of the total $1.43 million fiscal year 2008 performance fee allocated to physical security was associated with LANL's achievement of compliance-oriented milestones, such as issuing plans, publishing policies, and completing equipment maintenance requirements.

The management attention dedicated to improving physical security following the October 2006 thumb drive incident mirrors the level of attention that followed LANL's 2004 shutdown, when over 3,400 safety and security deficiencies were identified for correction. This shutdown lasted up to 10 months for some laboratory activities and cost as much as $370 million.[12] Given how quickly LANL's security performance declined between the full resumption of laboratory activities in May 2005 and the discovery of the thumb drive on private property, LANL's ability to sustain the improved security posture it has recently achieved is unproven. Strong federal oversight will help ensure that these improvements are sustained. However, we reported that the Los Alamos Site Office suffers from a shortage of security personnel and lacks funding needed for training. Specifically, as of October 2007, the Los Alamos Site Office employed 13 security staff—enough for 1 person to oversee each of the topical areas the Site Office had to evaluate. This staffing level, officials said, was sufficient to cover only 15 percent of LANL's facilities. In April 2008, a senior security official at the Site Office said security staffing levels had decreased since October 2007. Furthermore, while NNSA had identified the need to train and certify Site Office security personnel in specific subject matters, according to Site Office officials no specific training funds had been made available.

We made three recommendations to the Secretary of Energy and the Administrator of NNSA that, if effectively implemented, will improve physical security at LANL and help ensure that improvements LANL has achieved are sustained over the long term. Specifically, we recommended that LANL be required to develop a comprehensive strategic plan for laboratory security that addresses all previously identified security

[12]GAO, *Stand-Down of Los Alamos National Laboratory: Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered,* GAO-06-83 (Washington, D.C.: Nov. 18, 2005).

weaknesses and focuses on improving security program effectiveness. Furthermore, we recommended that NNSA provide meaningful financial incentives in future performance evaluation plans for implementation of this comprehensive strategic plan for laboratory security.

Preliminary Observations on Physical Security at Lawrence Livermore National Laboratory

In June 2008, the Committee requested that we review the security status at Livermore. This request came as a result of an evaluation by DOE's Office of Independent Oversight in April 2008, in which Livermore received the lowest possible ratings for protective force performance and for physical protection of classified resources. The evaluation also identified issues in other areas, such as security sensors and alarms, and security program management. We are currently verifying the findings of the evaluation and Livermore's actions to correct security deficiencies. Specifically:

- *Self-assessment and performance assurance testing programs at Livermore need improvement.* DOE's Office of Independent Oversight evaluations and Livermore Site Office security surveys found shortcomings in Livermore's fiscal year 1999, 2000, 2002, and 2008 self-assessment programs. In addition, Livermore and NNSA security officials acknowledged that a lack of comprehensive performance assurance testing was a significant contributing factor to the poor performance of Livermore protective forces during their April 2008 exercise. Between December 2006 and April 2008, Livermore did not hold an integrated performance assurance test of its protective forces or operationally test equipment key to the laboratory's protective strategy. During our visit to the laboratory 2 weeks ago, Livermore officials told us they are finalizing corrective action plans to address deficiencies in their performance assurance and self-assessment programs and have already conducted a significant number of performance assurance tests with the protective force and on equipment since the completion of the Office of Independent Oversight's 2008 evaluation.

- *NNSA and the Livermore Site Office have not always provided effective security oversight.* Six months before the Office of Independent Oversight's 2008 evaluation, the 2007 Livermore Site Office's annual security survey gave the laboratory a 100-percent satisfactory rating on its security performance, the highest possible rating. The results of the Office of Independent Oversight inspection not only differed markedly, but also found that the Livermore Site Office survey was not comprehensive and the ratings provided did not reflect what was actually observed. The Livermore Site Office is currently in the process of fundamentally

rebuilding and restructuring its survey program and has embarked on a training program for its security personnel.

Though our observations are preliminary, Livermore appears to be experiencing difficulties similar to LANL's in sustaining physical security performance. For example, in 1999, DOE's Office of Independent Oversight identified significant weaknesses in Livermore's programs to secure the laboratory's Category I special nuclear material facility against a potential terrorist attack. Livermore then embarked on a major program to improve security and, according to the Office of Independent Oversight, addressed most issues by 2002. This improved level of security performance appears to have been sustained through 2006. Between December 2006—when Livermore's protective force performed well in an exercise—and April 2008, security performance at Livermore declined. In response to the negative results of the 2008 Office of Independent Oversight evaluation, Livermore appears to be refocusing management attention on security performance.

While our work is preliminary, we believe the actions taken by Livermore, the Livermore Site Office, and NNSA, if and when fully implemented, will address identified physical security issues. However, just as at LANL, sustaining attention on physical security performance will continue to be a challenge.

Los Alamos National Laboratory Has Implemented Measures to Enhance Cyber Security on Its Unclassified Network, but Weaknesses Remain

LANL has implemented measures to enhance its cyber security, but weaknesses remain in protecting the confidentiality, integrity, and availability of information on its unclassified network. In particular, LANL has implemented a network security system that is capable of detecting potential intrusions on the network. However, LANL has vulnerabilities in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources. For example, although LANL had implemented strong authentication measures for accessing the network, these measures were not always used. Once a user successfully accessed the network, the user could create a separate, simple password that would allow alternative access to certain sensitive information. Furthermore, LANL neither conducted comprehensive vulnerability scans of the unclassified network nor included sensitive applications in these scans, thus leaving the network at increased risk of compromise or disruption. In addition to these weaknesses, LANL's

computing facilities had physical security weaknesses and could be vulnerable to intentional disruption. Specifically, we observed lax restriction of vehicular traffic entering the laboratory and inadequate fencing.

A key reason for the information security weaknesses we identified is that LANL has not yet fully implemented an information security program to ensure that controls are effectively established and maintained. Although LANL has implemented a security awareness training program, we identified a number of shortcomings in its overall information security management program. For example, (1) its risk assessment was not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the network security plan was incomplete, (4) system testing had shortcomings, (5) remedial action plans were incomplete and corrective actions were not always timely, and (6) the network contingency plan was incomplete and inadequately tested. Until LANL ensures that the information security program associated with its unclassified network is fully implemented, it will have limited assurance that sensitive data are adequately protected against unauthorized disclosure or modification or that network services will not be interrupted.

Many of LANL's cyber security deficiencies have been the subject of prior evaluations conducted by DOE's Office of Independent Oversight and the Los Alamos Site Office. The most recent reports, covering fiscal years 2006 and 2007, documented significant weaknesses with LANL's unclassified information security program, including foreign nationals' access to the laboratory's unclassified network. As of May 2008, LANL had granted unclassified network access to 688 foreign nationals, including about 300 from countries identified as sensitive by DOE, such as China, India, and Russia.[13] In addition, foreign nationals from sensitive countries have been authorized remote access to LANL's unclassified network. The number of foreign nationals who have access to the unclassified network has raised security concerns among some laboratory and NNSA officials because of the sensitive information contained on the network. According to LANL, the percentage of foreign nationals with authorized remote access to the unclassified network has steadily declined over the last 5 years.

[13]DOE identifies countries as sensitive based on national security, nuclear nonproliferation, or terrorism concerns.

NNSA and LANL have not agreed on the level of funding necessary for protecting the unclassified network. From fiscal years 2001 through 2007, LANL spent $51.4 million to protect and maintain its unclassified network. Although LANL cyber security officials told us that funding has been inadequate to address some of their security concerns, NNSA officials raised questions about the basis for LANL's funding request for cyber security. NNSA's Chief Information Officer told us that LANL has not adequately justified requests for additional funds to address the laboratory's stated shortfalls. In addition, NNSA officials informed us that LANL's past budget requests were prepared on an ad hoc basis and were not based on well-defined threat and risk assessments. In response to these concerns, in fiscal year 2006, NNSA implemented a more systematic approach to developing cyber security budgets across the nuclear weapons complex, including LANL. This effort, however, does not provide guidance that clearly lays out funding priorities. Furthermore, NNSA does not consistently document resource allocation decisions and identify how funding shortfalls affect critical cyber security issues.

To help strengthen information security controls over LANL's unclassified network, we made a series of recommendations to the Secretary of Energy and the Administrator of NNSA, 11 of which focus on improving LANL's information security program and determining resource requirements for the unclassified network. For example, we recommended that the Secretary of Energy and the NNSA Administrator require the Director of LANL to, among other things, (1) ensure that the risk assessment for the unclassified network evaluates all known vulnerabilities and is revised periodically and (2) strengthen policies with a view toward further reducing, as appropriate, foreign nationals' access to the unclassified network, particularly those from countries identified as sensitive by DOE. We made an additional 41 recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to identification and authentication, cryptography, audit and monitoring, configuration management, and physical security that we identified.

Mr. Chairman, this concludes our prepared statement. We would be happy to respond to any questions that you or Members of the Subcommittee may have at this time.

GAO Contacts and Staff Acknowledgements

For further information on this testimony, please contact Gene Aloise at (202) 512-3481 or aloisee@gao.gov; Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov; and Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Jonathan Gill, Ed Glagola, Jeff Knott, and Glen Levis, Assistant Directors; Allison Bawden; Preston Heard; Tom Twambly; Ray Rodriguez; John Cooney; Carol Herrnstadt Shulman; and Omari Norman made key contributions to this testimony.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Mr. STUPAK. Ms. Bowden, would you care to make an opening statement?

Ms. BOWDEN. No, sir.

Mr. STUPAK. OK. Let's begin our questioning then. Let's go 10 minutes and move it along.

Mr. Wilshusen, let me ask you this: I'm glad to hear that Los Alamos is doing better. This committee has really been on their case, because we have had so many hearings concerning their physical security. So we're pleased to see that.

We've asked in the past that GAO take a look at the need for a Los Alamos. In other words, there's a lot of redundancy in our labs. Is it necessary to keep that—is that investigation or report by GAO ongoing, looking at the physical assets of Los Alamos and is it needed?

Ms. BOWDEN. Yes, Mr. Chairman. We have finished the first part of that review, which was the report that was issued on physical security in June 2008. And we are just beginning the second phase of that review, which will take a comparative look at infrastructure across the nuclear weapons complex.

Mr. STUPAK. OK. Thanks.

Well, let me ask you this, Ms. Bowden, if I may. One of the concerns you raised in reporting on Los Alamos' physical security structure, that it seemed to be cyclical in nature. I'm glad to see that they're improving. But the labs appear to improve when we've had a mishap and they know they're under scrutiny.

How do we make sure there are improvements in the physical security, whether it's cyber or just physical security, unless this committee or—unless there's an incident, it seems like they regress. How do we break the cyclical nature of this?

Ms. BOWDEN. In our June 2008 report, we've recommended specifically that NNSA effectively incentivize financially, through newly established performance-based contracts, effective incentives for physical security performance. They get beyond compliance-oriented measures, but really look at the effectiveness of the security programs at Los Alamos.

In addition, we believe that effective security oversight through the NNSA site office will help address the sustainability of improvements in security at the laboratory.

Mr. WILSHUSEN. Regarding cyber security, it will take several things to make that happen. One, of course, is first getting the current control situation up to snuff in terms of—in particular, like implementing our recommendations over the weaknesses in its present controls. But that's only as a point certain.

It's also imperative that the Agency develop the processes and the structure to ensure that these controls and its risks are adequately assessed over time because the computing environment changes. The cyber security environment is very dynamic. There are constantly new threats, new technologies and new business processes and functionality that are being added to the unclassified networks and to any network, speaking generally. And so it requires that the Agency sets up the processes and effectively implements them over time.

Mr. STUPAK. Well, let me ask you this: To the extent that you can testify, you or Mr. Podonsky, in open session here, what is the

level of sophistication of these cyber attacks? And I take it they're increasing in capability.

It's getting much more sophisticated these cyber attacks, is it fair to say?

Mr. WILSHUSEN. Definitely, they're becoming more sophisticated and they're also becoming more targeted. In the past, many of the attacks were just through hackers or virus writers that might throw out a virus across the Internet and see what they might be able to infiltrate. Now attackers—and they come from a variety of sources—more specifically target their—well, they more specifically try to target their more particular systems or individuals that they want to attack; and they tailor that attack to try to encourage an individual to open up an e-mail attachment or to provide sensitive information, like personally identifiable information, or to go to a Web site to which can then be downloaded malicious software which can provide the opening to the attacker.

Mr. STUPAK. Mr. Podonsky, I think you actually said in your testimony that before instead of a straight-in attack, now they use a different method or go through someone who will already have access to it, get them to open an e-mail or whatever, and then make the attack.

Mr. PODONSKY. In my opening statement I did talk about the sophistication of these attacks. And I'm sure in the closed session we'll be able to talk with greater granularity.

However, I want to emphasize again, as I said in my opening statement, while DOE is a target, so is the entire United States Government.

Mr. STUPAK. Sure.

Mr. PODONSKY. And we need to be sensitive that these attacks are very real, not only against our laboratories, but against all of our agencies.

Mr. STUPAK. Well, and in my testimony, I had mentioned that tens of millions of attacks are taking place each month. Are we at a point where the number of attacks have outpaced our ability to defend against them, or to identify them when they do occur?

Mr. PODONSKY. In our opinion, from independent oversight, we believe that there are things that we can do to help protect some of the information that we have. But the reality is that these attacks continue to be, as you point out, more sophisticated and more numerous. And it's a constant, continuous struggle for all of us.

Mr. STUPAK. But you also mentioned in your testimony your Red Team and how you're able to penetrate two of the DOE labs and downloading a very large quantity—gigabytes, you said—of information.

Can you expound further on what your Red Team did? And what does this suggest about the capability of the Department of Energy to thwart cyber attacks?

Mr. PODONSKY. What I can say in open session, first, yes, I would like to explain in greater detail in a closed session what they actually did and the only reason I can say that is because we do not want to confirm for hackers out there what the successful practices are, because we've proven that within the Department.

But suffice it to say that, as I said, with a very small group of cyber security specialists, and in under, as I said, 90 days, we were able to take over the network of two of the sites.

We believe that were we with more people—and I'm not asking for more, but were we with more people and had we pursued this for a longer period of time, there would have been more vulnerabilities that we would have found.

Mr. STUPAK. I think, Mr. Wilshusen, and I think, Mr. Podonsky—I think you both mentioned it—the so-called yellow network, if you will, or the unclassified network at the labs is not sensitive enough to warrant major action to protect it. But yet these unclassified networks can lead you to terribly sensitive information; is that correct?

Mr. WILSHUSEN. Yes. Certainly the information on the yellow network contains very sensitive information, including unclassified controlled nuclear information, export control information, and personally identifiable information about LANL employees. This information has intrinsic value to attackers and to—of various different types.

It can be—information from a network potentially can aid our competitors, or provide a competitive advantage to—in the commercial sector. It can also be a source for intelligence gathering and possibly disruption for other adversaries.

And so certainly that information has value. And I think that's indicative, in part, by the number of attempted probes that occur at that site.

Mr. STUPAK. Well, you mentioned maybe the commercial nature of it. But what about national security? Does the information contained in the unclassified network pose a danger from an adversary by going through the yellow network or unclassified network? Can you get to something where an adversary, from a national security point of view, could penetrate and then cause us problems?

Mr. WILSHUSEN. Well, I would say that the type of information on that network could certainly aid intelligence operations from other organizations. It's highly sensitive and it could potentially lead to that, yes, sir.

Mr. STUPAK. Well, what's your opinion? And on the network access that's been provided to foreign nationals from both sensitive and nonsensitive countries, do you think that's too open to foreign nationals?

Mr. WILSHUSEN. Well, I think the issue relates to—it really comes down to a risk and benefit decision; you know, what is the risk of giving these individuals, particularly from the sensitive countries, access to the unclassified network; and then what's—first is, what is the benefit of giving them access to it?

And once it's decided whether or not these individuals should have access to it, it's incumbent then upon the organization to ensure that—as it would for any user, to ensure that the access granted to that individual is based on the principle of least privilege, and that they're only given the access that they need to do the job and no more, and that that access is based on need to know.

Now, we've been informed that the NNSA has decided to remove the access of all the foreign nationals from sensitive countries, from the yellow network.

Mr. STUPAK. OK. Because isn't it sort of like what we did in Los Alamos? I mean, I think we had a hearing on it where foreign nationals had access—many people thought too much—and then they just pulled back for the foreign national to limit the access at Los Alamos; am I correct?

Ms. Bowden or—do you know?

Mr. WILSHUSEN. You mean previously?

Mr. STUPAK. Right.

Mr. WILSHUSEN. That I don't know, sir.

Mr. STUPAK. OK.

Mr. Friedman, if I may ask one question. I don't want to leave you out there. Maybe we'll get around the second time.

In your January 2008 you reported that the Department failed to adequately address cyber security incidents, coordinations and communications. In our next panel Dr. Wilbanks will say just the opposite.

Why is there such a difference of opinion as to the effectiveness of cyber security incident coordination and communication? And why is this such a challenging area for the Department? And who within the Department is really responsible for collecting, reporting and disseminating cyber incident information?

In other words, I guess, who is responsible for the program? Why do we have such diverse views on how effective they're being on the cyber security?

Mr. FRIEDMAN. Well, Mr. Chairman, I can't speak to Ms. Wilbanks' testimony, and I'm not sure I can completely understand the distinction.

The Department does have a fairly sophisticated system of collection, both a NNSA system and a non-NSA system of collection of these incidents, in part to report to law enforcement, partially my office and others, and in part to do trending analysis and best practices and to alert the various facilities within the Department as to where the problems may be, and trends they may see that may affect all of the individuals.

What we found in the past is that these two entities, which by the way are in the process of being consolidated, at least in part, that they did not receive—we did not receive from them all the information that we needed to have a quality referral to law enforcement and we had to go back and get additional information.

So the structure is in place along the spectrum. The question is, is it as complete and comprehensive as it needs to be and as responsive to the needs of law enforcement and to the others throughout the Department?

Mr. STUPAK. OK. I thank you. Before I yield to Mr. Shimkus, you know, there has been this report or letter by Mr. Terry Turchie, and Mr. Dingell brought it up more in his opening statement. And I am sure you are going to be looking into that, the comments made in the letter by Mr. Turchie as to counterintelligence and the intelligence. Will your office be looking at that?

Mr. FRIEDMAN. Is that directed to me?

Mr. STUPAK. Yes.

Mr. FRIEDMAN. I first saw the letter from Mr. Turchie this morning at 10 minutes to 8:00 and I hadn't seen it previously. I had seen the report by the Congressional Research Service about 5 or

6 months ago, which addresses many of the same issues. We are certainly looking at it carefully and we will be considering what the next step should be.

Mr. STUPAK. We look forward to working with you on that, because we are going to look at cybersecurity at all the agencies under our committee's jurisdiction. So I just wanted to let you know. Thank you.

Mr. Shimkus for questions, please.

Mr. SHIMKUS. Thank you, Mr. Chairman. Still being relative new to the committee and the oversight, having been on the full committee for a long time, I don't come with the years of analysis and frustration that many members do in delving into this.

But current events dictate internationally that if a cyber red team, given a month and six to seven folks, can do great mischief, it poses a question, what can a nation state do with unlimited people and really unlimited dollars? In the international arena we have seen it with Estonia, we have seen it most recently in Georgia, not the State but the country.

So it begs the question, if there is information, whether it is technical in nature or that can be combined on this yellow network, that is, quote/unquote, sensitive and all these words are—if it is sensitive, either personal information or it can then be placed together to create other information, that is I think a problem.

And also, if in this definition of sensitive information and that information then runs the risk of—well, let me say it this way. In a communication environment, as we talked about before, you have got information available for doing the job, there is risk entailed. Are we willing to take the risk? Are we willing to assume the risk? I understand there is an open green—kind of like a green system which we can go to the general information on DOE, then the yellow system, and then the more—the issue that is classified. How do we clean up the yellow network so that the classified information isn't there and it is not accessible through the other networks? And let me go to Mr. Wilshusen first.

Mr. WILSHUSEN. Well, I think, first of all, with regard to the information on the yellow network, classified information is not authorized to be on that network. And so there has to be a process that goes through to make sure that information that is on that network is not classified. And so there is some classification requirements on that to assure—determine whether or not somebody that is on the yellow network can gain access to the red network. Is that what you are asking?

Mr. SHIMKUS. Or green to yellow to red.

Mr. WILSHUSEN. Right. Well, we are—

Mr. SHIMKUS. And then is part of that the Trojan Horse part of thing that you're talking about is accessing in and then sleeping and then awakening and then moving through aspects?

Mr. WILSHUSEN. Right. We are, at the request of this subcommittee and the full committee, reviewing the security controls over the classified network at Los Alamos, too. So I can't comment on that at this point in time. Our work is still premature to make any type of preliminary information or observations on the security controls over the red network.

However, with regard to the yellow network and the green network, they were interconnected in the past, and that was one of the issues that we have identified that weaknesses—even though our work on this particular engagement focused on the yellow network, we found that there were paths from the green network into the yellow network.

Mr. SHIMKUS. And then I would ask if that was identified, have those paths then severed that we know of today, that interconnect—the interconnection, the ability to do that?

Mr. WILSHUSEN. You mean today is that capability, do those weaknesses still exist?

Mr. SHIMKUS. And that is probably a question for Mr. Friedman and Mr. Podonsky. But, again, I have been on the telecommunications, the tech committee and stuff, but I think the only way you can really—information gets compromised in one or two ways. You either have hackers that can use the system to move through, so you have to sever the connection. Or you have actually humans who surreptitiously, illegally, as in flash drives, grab information. And we know that has happened in the past, too.

So that for security aspects, one would be sever the connections on the green network so that it does not have? And that is what you recommended. And the question would be to Mr. Podonsky and I guess Mr. Friedman, your analysis. Has that happened? And can it? Or can you not do the mission if you do that?

Mr. PODONSKY. So far, Congressman, we have never identified any pathway from the green to yellow network. However, we strongly believe that the yellow network that we are referring to, which varies from lab to lab and site to site in terms of what goes on there, the certification and accreditation process that is part of the Department, and Mr. Friedman talked about, is there to make sure that we look at some of this sensitivities of these networks.

While my colleague from GAO mentioned that there is no classified, or supposed to be, on the yellow network, the fact of the matter is we do need a classification process for classified information.

The labs also do need a sensitive process. We need better controls. There is no doubt in our minds from the oversight perspective that while the information is not classified but is sensitive, that doesn't mean it is not valuable to somebody. And that is what we are concerned about. But we also believe, as I said in my opening statement as well as the written testimony, that we believe there are things that we can do, like encryption of the information that is on the network.

Mr. SHIMKUS. The yellow system, can they e-mail outside of the system? If you are on the yellow network, can you e-mail to like Berkeley or the country of Georgia? And if you can, is that then a main pathway of concern?

Mr. PODONSKY. Yes, it is. And they can. And one of the things I mentioned, and I want to reiterate my point in my opening statement, is that we need to make tighter controls on making sure that if somebody who is unauthorized into the yellow network cannot send the information out the way our red team did. And there are mechanisms that can be used by the Department to prevent that as best we can.

One of the other problems is at Los Alamos, for example—and it is not unique to Los Alamos and it is not unique to DOE, I can emphasize—is that when you have 25,000 individual laptops or stand-alone computers and these people are cleared to use those, there is also a trust factor. And we have seen at all the sites within the Department sometimes that human factor fails. So what we do need is we need systems in place to put tighter controls.

Mr. SHIMKUS. I am just trying to do a comparable to our systems here. We have the Web sites, we have the e-mails. There are some firewalls that disallow individuals from e-mailing us unless they kind of identify that they are from the constituency, and there is a blocking portion of that. I am not sure if that is off-the-shelf type—of probably not very—because we really don't handle sensitive—it might be sensitive politically or for other purposes, but not to the extent that this is. This is of a concern.

So I would—that would be where I would follow up, is trying to make sure that the individuals are well-screened and we do the background checks. Foreign nationals is a concern. And the risk, the whole question of risk and reward based upon the available information and the work that foreign nationals can do.

So, again, this is my first oversight investigation hearing on this subject. I know this committee continues to be very diligent. We have had really bad case scenarios in the past. And I just pledge my support to the chairman to be engaged with him as we move forward. And thank you for your time.

Mr. STUPAK. I appreciate that. I appreciate the gentleman's comments.

If I just may. On this yellow that you were talking about, yellow network. Information out there may be unclassified. But if I take a piece of yellow unclassified, put it with another piece of yellow unclassified, put it together, that information then could become classified. Is that?

Mr. PODONSKY. If I can, Mr. Chairman. We call that the mosaic effect. And I would say it is counterintuitive to think that there is not a value of the information on the network. It is speculative for any of us to say that it would actually fit together and become classified. But irrespective of whether it is classified, the sensitivity can be of extreme value to people who mean to do harm to our Nation. It may not be in the realm of national security information, but let me give you an example.

We sometimes send things that's password protected. We'll send a message, and then it will be followed up by another message that has the password in it. So if—I am not from the Intelligence Committee, but if somebody is vacuuming up all the information they can, they can put those two together and get that password protection. Again, it's not classified, but it's sensitive enough that we need to have stronger controls in place.

Mr. STUPAK. Mr. Friedman.

Mr. FRIEDMAN. Mr. Stupak, first of all, the mosaic effect is important. And you described it well, I think. But one of the problems with the yellow network, and it's not—it's understandable and it's the nature of the contents of the network, is that—and if you recall, if I might divert you for a second. In 2005 or 2006, we had

the exfiltration of PII, personally identifiable information, at the Albuquerque Service Center, I believe.

One of the problems is that this information, while it may not be classified, if it falls into the hands of the wrong individual, that individual could conceivably be exploited by an inappropriate source. So there are—it's sensitive information that needs to be carefully protected.

Mr. STUPAK. Mr. Dingell for questions, please.

Mr. DINGELL. Mr. Chairman, I thank you. Mr. Chairman, first I would like to insert in the record a letter received by me from Mr. Terry D. Turchie, which pretty much speaks for itself about the situation with regard to security at the Lawrence Livermore National Weapons Laboratory. I will have some questions about that after I finish my first set of questions and perhaps some later time.

These questions, yes or no. Mr. Podonsky, in your testimony you mentioned one of your most recent red teams was able to penetrate the networks of two DOE labs. Is that correct?

Mr. PODONSKY. That is correct, sir.

Mr. DINGELL. Which were those?

Mr. PODONSKY. They were two science labs.

Mr. DINGELL. You don't want to identify them by name?

Mr. PODONSKY. I am happy to identify those in executive session, sir.

Mr. DINGELL. Thank you. Mr. Podonsky, isn't it true that your red team was able to download very large quantities; i.e., gigabytes, of data, some of which were sensitive, without being detected by DOE authorities?

Mr. PODONSKY. Yes, sir.

Mr. DINGELL. Mr. Podonsky, you also indicated that the level of access your team was able to quickly obtain over the course of just a few months would have allowed you to change data or otherwise corrupt a particular lab's cyber network. Isn't that correct?

Mr. PODONSKY. Yes, sir, it is.

Mr. DINGELL. Mr. Podonsky, I am gathering what your red team did to these labs' cyber networks has rather profound security implications. Is that correct?

Mr. PODONSKY. Yes, sir, it does.

Mr. DINGELL. Mr. Podonsky, doesn't this suggest that the DOE does not currently have sufficient capability regarding its cyber defenses.

Mr. PODONSKY. No, sir, it does not.

Mr. DINGELL. What, in your words, does this exercise suggest as to the capability of DOE and its labs to thwart cyber attacks?

Mr. PODONSKY. What it tells us, Mr. Dingell, is that we have some of our sites that are inconsistent in their application of DOE policies. We have some sites that perform better. But, overall, the Department of Energy as the rest of the government has to strengthen our cybersecurity networks.

Mr. DINGELL. Mr. Podonsky, isn't it true that the addition to the access your team gained at these two sites, by installing your own malicious programs on a number of their laptop computers your red team was able to make important footholds into the networks of other facilities after these laptops were legitimately connected to their respective networks?

Mr. PODONSKY. Yes, sir. That is correct.

Mr. DINGELL. Mr. Podonsky, moreover, didn't additional activity conducted by your red team demonstrate your team's ability to possibly move around throughout a number of DOE sensitive networks?

Mr. PODONSKY. We believe that that would have been the case if we had continued on with the activity.

Mr. DINGELL. What more can you tell about that?

Mr. PODONSKY. Well, we terminated our activity because we were aware that there was actual infiltration in some of the sites that we were looking at.

Mr. DINGELL. Now, Mr. Wilshusen, yes or no again, please. Some have suggested the information on the yellow unclassified network at the labs is not sensitive enough to warrant major action to protect it. This is a question that our chairman has been raising on this. I gather you don't agree with that statement.

Mr. WILSHUSEN. That is correct; I do not agree.

Mr. DINGELL. Now, Mr. Wilshusen, in fact your reports say that the information in the Los Alamos unclassified network contains such information as Naval propulsion data, personally identifiable information, unclassified controlled nuclear information, and a host of other sensitive categories of information. Is that correct?

Mr. WILSHUSEN. That would be those categories of information. Yes.

Mr. DINGELL. Could you mention any other categories that should be addressed?

Mr. WILSHUSEN. Did you include our unclassified controlled nuclear information?

Mr. DINGELL. Yes.

Mr. WILSHUSEN. OK.

Mr. DINGELL. Mr. Wilshusen, isn't it the case that your report said that that kind of information a valuable target for foreign governments, terrorists, and industrial spies?

Mr. WILSHUSEN. Yes.

Mr. DINGELL. Mr. Wilshusen, I gather that GAO does not believe, given your findings at the labs, the DOE as a whole is sufficiently prepared for cyber attacks or cyber intrusions. Is that correct?

Mr. WILSHUSEN. I would say that they are at increased risk. Yes.

Mr. DINGELL. And that would be a substantial risk?

Mr. WILSHUSEN. It could be. Yes, sir.

Mr. DINGELL. Now, Mr. Podonsky again. Let's talk about—let's talk about this. The Director of Los Alamos remarks in his testimony that your offices draft audit report for August/September recognizes that Los Alamos National Laboratory is making progress in many security areas. Is that correct?

Mr. PODONSKY. That is correct. They are making improvements that we have not seen in 20 years.

Mr. DINGELL. But I gather, however, that the lab is still not out of the woods when it comes to physical security. Is that correct?

Mr. PODONSKY. There are areas that they need to improve upon, but they have made quantum leaps from our last inspection.

Mr. DINGELL. Ms. Bowden, isn't it true that DOE's Office of Independent Oversight found major concerns regarding Lawrence Livermore's security capability in April of this year?

Ms. BOWDEN. Yes, sir.

Mr. DINGELL. Ms. Bowden, in your testimony you say concerning the exercise that, and I quote, "Livermore received the lowest possible rating for protective force performance and protection of classified resources." Isn't that correct?

Ms. BOWDEN. Yes. That is what the Office of Independent Oversight found.

Mr. DINGELL. And, GAO, to the extent that you can identify this in an unclassified setting, how did Lawrence Livermore get into this position and what are the root causes?

Ms. BOWDEN. Well, in a general sense, and based on our preliminary observations, because this work is ongoing, we discussed that question with officials at the laboratory and with officials—Federal officials at the site office. And there are a number of factors that may have contributed, though we will continue to work on this.

Those included focus—a focus shift on contract transition, the declaration of the site as non-enduring for Category I special nuclear material. And, in addition, frequent security policy changes over the different design basis threats that had been issued over a period of time.

Mr. DINGELL. Thank you.

Mr. Podonsky, it was your claim that GAO referred to in their testimony as doing the physical red teaming of Lawrence Livermore. Is that correct?

Mr. PODONSKY. Yes, sir.

Mr. DINGELL. Mr. Podonsky, I have limited time so I know you will speak quickly. But tell us how you believe Lawrence Livermore got into the posture where it has performed so poorly.

Mr. PODONSKY. It's a mystery to us, Mr. Dingell, because we have seen in our last inspection before the spring that they were performing well. We do believe that a great contributor is, as the GAO just mentioned, having to do with the contract change-out.

Mr. DINGELL. Ms. Bowden again, if you please. One of the concerns you have raised in your report about Los Alamos's physical security posture is the cyclical nature. What—that is, the labs appear to improve when they have had a mishap and know that they are under scrutiny. Is that correct?

Ms. BOWDEN. Yes, sir.

Mr. DINGELL. Ms. Bowden again. What explains the root cause of the cyclical nature of the security at the labs, and how can we prevent this?

Ms. BOWDEN. In our report we have made several recommendations that we think will address sustaining improvements over time, the first of which is providing better financial incentive for effective security performance in the contract determinations for the award fees at the end of each fiscal year. In addition, we feel it's important to ensure adequate NNSA site office oversight of security on a consistent basis at the laboratory.

Mr. DINGELL. Mr. Chairman, because of the limited amount of time, I request that this letter be inserted in the record, and I would ask that our witnesses give us their comments on the findings and the statements made in the letter, and I would ask that the record be kept open so that that may be inserted into the record at the appropriate fashion in time.

Mr. STUPAK. Without objection. I would also note that it's in our binder. So it will be made part of the record, Mr. Chairman.

[The information appears at the conclusion of the hearing.]

Mr. DINGELL. Thank you, Mr. Chairman.

This to Mr. Friedman. The Federal Information Security Management Act requires that the Office of the Inspector General conduct an independent annual evaluation to determine whether the Department's unclassified cybersecurity program properly protects its information systems. Is that correct?

Mr. FRIEDMAN. That is correct.

Mr. DINGELL. Mr. Friedman, in 2008, your evaluation report of the Department's unclassified security program states: The Department continues to make, quote, incremental improvements in this program. Yet, isn't it true that you have continued to find ongoing concerns with DOE's cyber defense capability?

Mr. FRIEDMAN. That is correct.

Mr. DINGELL. Mr. Friedman, in fact, isn't it correct that your latest reports found the following over the past few years: Unsolved issues surrounding risk assessments and adequacy of security controls? Yes or no?

Mr. FRIEDMAN. You are correct, sir.

Mr. DINGELL. Lack of centralized department-wide inventory of information systems.

Mr. FRIEDMAN. That is correct.

Mr. DINGELL. That is a fairly simple to do, isn't it, to perform that particular act?

A failure of some sites to complete contingency disaster plans.

Mr. FRIEDMAN. Correct.

Mr. DINGELL. Failure of Department officials to implement Federal and Department security requirements in a timely manner.

Mr. FRIEDMAN. That is correct.

Mr. DINGELL. Mr. Friedman, in your opinion, do these weaknesses continue to exist?

Mr. FRIEDMAN. They—our reports are current. And the answer to your question, Mr. Chairman, is that until we do another review and see that they are not in effect, we will continue to believe that they exist. Yes.

Mr. DINGELL. Now, why do these security questions and weaknesses continue to exist?

Mr. FRIEDMAN. That is one of the most perplexing questions that I deal with every day, Mr. Chairman.

Mr. DINGELL. It seems to be a leadership problem. Doesn't it?

Mr. FRIEDMAN. Well, I would say this. The conclusions that we reach after thinking about this over a great deal of time is that the Department lacks the ability to close the game, in the sense that a lot of good actions are initiated but they don't get completed and implemented. And that seems to be a problem.

Mr. DINGELL. Thank you.

Mr. Chairman, I appreciate your courtesy. Thank you.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. Burgess for questions.

Mr. BURGESS. Thank you, Mr. Chairman.

Let me ask a question to the GAO related to the management of the money available for security. How much money have we allocated for overseeing that security's implemented and followed?

Ms. BOWDEN. In fiscal year 2007, it was about $188 million.

Mr. BURGESS. And so that is not a huge sum by Washington standards, but a significant sum, and the problems persist. What sum is it going to take so that we get to the place we want to be?

Mr. WILSHUSEN. That is a very difficult question to answer, and I don't know if I can point to say this is the sum that is needed. I think what I can say, though, is that the agency needs to properly assess its risks and determine what policies and procedures that they need to implement to cost effectively reduce those risks to an acceptable level.

We have to remember that security is a risk management problem; it's not a risk elimination or risk avoidance problem. Because you can throw so much money at security and you can lock down everything, but at the same time the costs would be prohibitive as well as it will probably take a major hit on productivity. So it's really a balancing act to determine how much is necessary to secure the systems based on risk.

Ms. BOWDEN. And if I may clarify, the dollar figure was for Los Alamos.

Mr. BURGESS. But we are going to have—it will be budget time again before we know it, and we are going to have to be thinking through these things. At some point we are going to need some advice from people like you as to whether or not we are doing our job in providing you the resources; i.e., the funds that you need to hire the personnel, to purchase the software, to run the red teams, to make sure that things happen the way that they are supposed to happen.

Mr. WILSHUSEN. Well, certainly what I will say, too, is that for many of the recommendations that we are making in our reports that are being released today, much of that would not necessarily require additional acquisition of software devices. It's more of a management issue, taking the security controls, the devices that are presently there, and configuring them in such a manner to make them more secure.

Mr. BURGESS. We may come back to the management question in just a moment. But is it also a matter of time?

Mr. WILSHUSEN. Yes, sir. Time is of—in our view, time is of the essence in terms of taking the corrective actions to improve the security over the unclassified network at Los Alamos, because of the sensitive information it contains and because of the risks associated with the weaknesses that we have identified.

Mr. BURGESS. Well, giving you more time may increase the risk. Providing you more money, if you can do it in a shorter period of time, in my mind at least, would be a reduction of risk. I am just not sure how much. I am not sure how much flexibility we should be willing to give on time for implementation just because of the risk that is out there. I mean, and it's not just you, but certainly your area is—it's such a significant vulnerability that we really can't overlook it.

A question, Mr. Podonsky, about the number of laptops. What was the number that you told us, the number of laptops that may move around?

Mr. PODONSKY. I misstated. I was meaning the stand-alone sets of computers, which I said were 25,000 users at Los Alamos. And I used that example to answer Chairman Stupak's questions about the vulnerability of the yellow network.

Mr. BURGESS. What would be the correct figure for the number of laptops that may move around in so-called trusted circles within the lab?

Mr. PODONSKY. I don't have that number. I would have to get that number and get it back to you.

Mr. WILSHUSEN. One of the things that we've identified on our review was that there are about 13,000 users. Now, this is just on the unclassified networks, so I can't comment on all of the networks at Los Alamos. But just for a scope. There are about 13,000, a little bit over 13,000 users on the unclassified network, and that network contained about 25,000 devices. And so those would include work stations, but also routers, switches, and other types of devices.

Mr. BURGESS. But as we have seen from these reports and other areas, a misplaced laptop is a source of great vulnerability. And all of us, you and us, are under great scrutiny in that regard to make certain that these very powerful and very useful devices—they can certainly increase productivity but they really expose a great deal of vulnerability if we are not careful. So I just wonder if we shouldn't be a little bit more circumspect about the number of devices that are actually out there with information.

I think it was on this panel that we heard about the purchase of some of the equipment, which is proprietary equipment, with USB ports that might be vulnerable to access. And we sealed them up with JB Weld—which is a good Texas product, so I am glad but we used J Weld, but it just seemed like a significant oversight in the purchase of that equipment to lead us to that degree of vulnerability. And then laptops that can move around so easily and be left somewhere or stolen or lifted, or even if someone did have an idea to do something that they shouldn't be doing, it just makes it that much easier for the person who has a criminal intent.

I guess, Mr. Podonsky, this is for you. On the issue of—I think we've talked about this before on this subcommittee, about this issue of encryption and sequestration. How is that project going? Where are we with that? Can you develop that a little bit for us on the sequestration and the equipment side?

Mr. PODONSKY. What I can tell you—first, I am sure the second panel can give you more clarity on how far they have gone in that arena. But from our inspection process, we don't feel that enough of the sites are encrypting the information that needs to be encrypted. There is—

Mr. BURGESS. Why is that?

Mr. PODONSKY. Well, because the policy says it is preferred that the information be encrypted. And we have learned over time that unless there is a regimented language that says you shall encrypt it, then using the word "preferred" becomes accounting option. And we find that a little disturbing.

Mr. BURGESS. Too much flexibility, in other words?

Mr. PODONSKY. That is what we believe.

Mr. BURGESS. Now, is there any problem with obtaining the software or the type of software that is available? Is there a satisfactory program that is out there that you all are using for the encryption?

Mr. PODONSKY. I believe the software is out there; but I also understand that the process would be a little bit less convenient when doing business.

Mr. BURGESS. And what about the sequestration aspect of it?

Mr. PODONSKY. I will have to defer to the CIOs.

Mr. BURGESS. And I think it was your testimony where you said the attacks were becoming more sophisticated, more targeted. Are they also becoming more frequent?

Mr. PODONSKY. Yes, sir, they are.

Mr. BURGESS. And do we have a general idea of where they are coming from?

Mr. PODONSKY. I think that is a question that really should be answered in the executive session.

Mr. BURGESS. Fair enough. We will do that.

A question was asked about what caused the lower security level at Livermore, and I think you answered, Mr. Podonsky. But Ms.Bowden, do you have an opinion on that as well through your study?

Ms. BOWDEN. I think we both agree that there was a shift in focus to the contract, the management and operating contract transition.

Mr. BURGESS. And that is at Livermore?

Ms. BOWDEN. Yes.

Mr. BURGESS. Because at Los Alamos, we had the contract evaluation but we didn't change the contract. Correct? Do I remember that correctly?

Ms. BOWDEN. The contractor was changed in 2006.

Mr. BURGESS. At Los Alamos?

Ms. BOWDEN. Um-hmm.

Mr. BURGESS. So when we talked about some of the leadership problems as that, do you think that has been dealt with satisfactorily?

Mr. PODONSKY. Sir, I would like to answer that, having inspected Los Alamos for the last 24 years. The answer is absolutely we see a sea change that we haven't seen there before. I just came back from the Los Alamos inspection closeout for my independent oversight, and we have seen a lot of improvements. We have seen commitments that we don't think were just pabulum. And we believe it's because of the accountability. We know that they are watching our enforcement actions and compliance orders. We know that they are paying attention to the inspections.

Mr. BURGESS. And do you think that there's going to be a way to extrapolate those successes to, say, the Livermore facility?

Mr. PODONSKY. I am sorry?

Mr. BURGESS. Is there going to be a way to extrapolate those successes to other facilities where we've fallen behind?

Mr. PODONSKY. Based on the aggressiveness by which the Livermore folks are addressing our very serious concerns from the

spring inspection, we are hopeful. But, again, the sustainability is going to be an issue that we are going to be watching.

Mr. BURGESS. Very good.

Thank you, Mr. Chairman. I'll yield back.

Mr. STUPAK. I thank the gentleman.

Ms. DeGette for questions.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

I would like to follow up on some of the questions that Mr. Dingell was asking. The first one being, on this yellow network, the unclassified network, there is still sensitive information. And everybody has agreed with that here today. And the question is, what dangers do we have if people can access that information? Because even though it's not classified, it still is important. Mr. Dingell mentioned a couple of the nuclear issues, but I just want to go through the list that the GAO listed in their report because it's really kind of shocking.

Business proprietary information. The nuclear information he talked about. Export control information. The military critical technology list. Confidential foreign government information. And personally identifiable information, including names, aliases, Social Security numbers, and biometric records of employees, contractors, and visitors.

Now, a lot of this information if someone were to access it would be criminal and even worse. This is not just completely neutral information. And so I have some follow-up questions on what is happening to try to preserve that information.

I guess my first question would be maybe to you, Mr. Podonsky, is do you think that the labs or the DOE have the technical expertise and resources to protect this information that is currently residing on the unclassified networks?

Mr. PODONSKY. Congresswoman DeGette, we do believe that the technical expertise exists within the laboratory community as well as with the rest of the Department. We do also believe that the sensitivity—we share your concerns about the sensitivity that is on the yellow network. That is why I have said in my testimony and in my opening statement we do believe tighter controls are necessary.

Ms. DEGETTE. Well.

Mr. PODONSKY. If I might continue. As exemplified by our red teaming effort, and we are not the most sophisticated red teaming hackers in the world, but given our capabilities and what we were able to do, that should give us all pause as to what we need to do.

Ms. DEGETTE. I was going to ask that question in a minute, because unlike my friend, our ranking member, I have been on this committee for 12 years and I have been to Los Alamos and I have been in these hearings and we have you guys down all the time. And every time you come in, you say, you know, we have these risks, we have these problems. It's always cropping up some other place. So if we have got the expertise and capability to do it, here's my simple question to you, why aren't they doing it? Because you are right, it's not just the yellow information, it's the red information.

Mr. PODONSKY. I can give you an opinion from oversight as to why the Department is not doing it.

Ms. DEGETTE. I would love that opinion.

Mr. PODONSKY. And our opinion is it's not always been the highest of priorities from different administration to different administrations. I would also say—

Ms. DEGETTE. But we have had this administration now—do you mean Washington administration or lab administration?

Mr. PODONSKY. No. Washington administration.

Ms. DEGETTE. Well, we have had this administration 8 years.

Mr. PODONSKY. In 2000, ma'am, we came to the floor of this hearing room and gave a demonstration, a live demonstration of how we could crack codes of passwords.

Ms. DEGETTE. I remember it. I was there.

Mr. PODONSKY. So we know that these problems exist.

Ms. DEGETTE. So why—we have had this administration 8 years. Is your testimony today that it has been a low priority for this administration? Yes or no?

Mr. PODONSKY. No, ma'am.

Ms. DEGETTE. Then why haven't we done it?

Mr. PODONSKY. I don't have a complete answer for you because I am not within the CIO's office. That is in the next panel. But from our perspective, we have written reports on this very subject multiple times.

Ms. DEGETTE. I am frankly, with all due respect, I am not particularly interested in the written reports. I am interested in when are we going to do this. If we have got the technical ability to do it, if we've identified the problem, then how quickly could we solve the problem if appropriate attention were given? Anybody can answer that if you know the answer.

Mr. PODONSKY. I don't know what my colleagues on the panel think, but I think this is a problem that can be solved.

Ms. DEGETTE. No. How soon can it be solved?

Mr. PODONSKY. As soon as the resources are applied.

Ms. DEGETTE. OK. So it's a resource question. That goes back to Dr. Burgess' question, which is, what kind of resources are we talking about here?

Mr. PODONSKY. We're talking about dedicated people within the cyber community to solve the problems.

Ms. DEGETTE. How many dedicated people? How much money?

Mr. PODONSKY. I would have to—without just giving it off the top of my head, I couldn't tell you that. But I think that we have—

Ms. DEGETTE. Do you know that?

Mr. PODONSKY. I believe we have it in the Department. We have the technical intellectual capabilities and we have the resource capability to make the changes.

Ms. DEGETTE. All right. So if you could supplement your answer within 30 days, I would appreciate it, telling us what kind of resources we would need to give to this.

Now, let me ask another question. And again if other people know, please chime in. Do we, if we have got the ability to do it and it's just a matter of resources and priorities, do we have a full inventory of all the information that is residing on these unclassified networks?

Mr. PODONSKY. I don't believe that we have a complete inventory on what resides.

Ms. DEGETTE. Is that something we would need to do?

Mr. PODONSKY. That would be a major undertaking for millions and millions of documents. And I am not so sure, Congresswoman DeGette, that that is the best use of the monies. The best use of the monies is to protect the information from going out, and protect the information from having access by hackers.

Ms. DEGETTE. It would probably also be worth reviewing categories of information to see if we really do need to have that on our networks then if we can remove it. Correct?

Mr. PODONSKY. Yes, ma'am. And that would be up to the individual program offices as to what types of information they are allowing their folks to put on the network.

Ms. DEGETTE. Well, maybe not. Because for some of these types of information, you could probably make a decision from the top whether you needed to have that information on certainly unclassified yellow networks. Information like aliases and Social Security numbers and biometric records of employees. It's hard to see how you would need to have that on some kind of a network. What do you think?

Mr. PODONSKY. Well, I don't know how they use all the information, but I do know they use that network to conduct business. And they separate that from the classified.

Ms. DEGETTE. See, what I worry about, though, is if you are leaving it up to each individual department head, that then you have no overall standard by which they could weigh it. So if you had an overall standard, then they could come in and ask for an extension if they had a need to put that on the network.

Mr. PODONSKY. And the CIO when he came on board in 2005, I believe, or 2006 put together with the three undersecretaries a governance model of federalizing the federation of policy that has the overarch policy, and then NNSA, Science, and Energy are able to tailor that to what their individual missions are.

Ms. DEGETTE. Now, Mr. Podonsky, do you think that the DOE lab should consider removing certain information on the unclassified network or increase its level of classification?

Mr. PODONSKY. As I said, Congresswoman DeGette, the laboratories need to take a good look, and the Department, in making sure that there are stronger protections of that information. Some of that information may need to be removed. But one of the problems is, where do you put it? If you put it on the classified net, you have now redefined what classified is.

So I again go back to our oversight perspective, is we need to keep people out of it, and we need to make sure that we have a rigorous process to make sure that anybody that might get in it cannot send information off the net.

Ms. DEGETTE. What is your opinion on that, Mr. Wilshusen?

Mr. WILSHUSEN. Well, I think I would also agree to the point that the information on that yellow network, whether or not that should be upgraded, if you will, and then reclassified and then put on the red network is a decision that is whether or not that information is classified or not. And that is something that needs to be done, and it probably has already been done, you know, it's been determined to be sensitive but unclassified. That is why it's on the yellow network.

But I agree with Mr. Podonsky, that the first thing that needs to be done is to better protect the information that is on that network by—

Ms. DEGETTE. I want to ask you one more question. Do you think there is some argument to be made about maybe making an intermediate network between the yellow and red networks for some of this unclassified information? You don't want to be calling things, as Mr. Podonsky rightly says, you don't want to be calling things classified if they are not. On the other hand, there is things that might be sensitive, like employees' Social Security numbers that are not necessarily classified information.

Mr. WILSHUSEN. Right. And because of that, such as personally identifiable information needs to be protected. But should that be on a different network? That is what the yellow network is for; it's the unclassified protected network.

Ms. DEGETTE. So your view is we need to protect that network better.

Mr. WILSHUSEN. Yes, ma'am. And—

Ms. DEGETTE. I just want to say, I know you folks can't make the rules, you can only make the recommendations. And I am sure that—you don't have to answer this, I am sure that many days you are just as frustrated as we are; you keep identifying these problems but yet no progress is made. So I want to thank you for your commitment to these issues. They are very important.

Mr. WILSHUSEN. Thank you.

Mr. STUPAK. Mr. Shimkus has a quick question, and then we will go on to Mr. Inslee.

Mr. SHIMKUS. And I will be brief. One thing I wanted to follow up with what I didn't was just an overall assessment of the corporate culture, or the culture of these labs and this whole issue. I agree with Chairman Dingell that it's leadership, and its leadership goes from the top and then the director of the lab, the director of the sub environments.

Has the corporate—let me, Mr.Wilshusen first. Has the corporate—did you evaluate the culture of the labs? And with respect to my colleagues who have been on this issue for a long time, which again which I haven't, has the culture changed positively in the security environment for the labs?

Mr. WILSHUSEN. Well, related to just the cybersecurity portion of it, and I will defer to Ms. Bowden on the physical security, we have just completed our review, and that is our first review that we have done reviewing cybersecurity out at Los Alamos. We have noted that some of their technical folks in terms of technical security individuals are among some of the better ones within the Federal Government. And, indeed, they implemented many innovative techniques to try to secure their unclassified network. However, we also found though that there were still a number of very significant vulnerabilities that impaired their ability to adequately protect that information on their network.

But in terms of the culture, I think there has been a change over the last year from what we have seen during the course of our audit. It seems like they are more concerned about the cybersecurity. But whether that is in response to our initial field

site visits and how long that remains, of course, remains to be seen.

Mr. SHIMKUS. Mr. Friedman, can you respond to that?

Mr. FRIEDMAN. Yes. In all fairness, while we still find problems and there are still concerns, and lot of them are serious, I don't think there is any question that the results of our work suggests, and our interactions with the laboratory personnel, that there has been a change in mindset, much more aggressive in the area of security. It may be beyond their capability to fix all the problems, but I think—and I have been observing this, sir, for three decades—there is a change. There is no question about that.

Mr. SHIMKUS. Thank you. And I would just hope that the position would be—I am not going to ask Mr. Podonsky to follow up, but I would just say, if there is a positive change in the culture, we need to push hard to sustain that change.

Thank you, Mr. Chairman.

Mr. STUPAK. Thank you.

Mr. Inslee for questions, please. 10 minutes.

Mr. INSLEE. Thank you. There has previously been a letter entered into the record from Mr. Terry Turchie that discloses very significant concerns by him. He's formerly with the FBI and he served as senior counterintelligence officer at Lawrence Livermore Nuclear Weapons Laboratory. This letter is dated September 1, 2008. And basically the letter is intended to alert Congress, it's a letter to Chairman Dingell, of what he considers very serious failures to focus on counterintelligence.

He describes there being a significant change from an emphasis or at least a significant commitment to counterintelligence to simply what he considers intelligence gathering. And he outlines in his letter quite a number of occurrences that would suggest there has been, at least in his view, a significant reduction in counterintelligence as he would define that activity. That, to me, is a significant issue, and I just would ask for the comment of any of you to respond to those concerns.

I want to note, too, that there are many people that are disgruntled with Federal activity. This is a gentleman who seems to have credibility, his resume is pretty outstanding, and I think his concerns ought to be ones that we would investigate. So I would ask for any of your response, I don't know if you have seen the letter, could respond to the general issue he has raised. His letter in general discusses a lack of financial and organizational commitment to counterintelligence as opposed to just what he would consider intelligence gathering. I just would ask for your comments, if you can provide them.

Mr. PODONSKY. The only thing, Congressman, that I can tell you is that, number one, I have not seen the letter. We do work with the intelligence and counterintelligence office, and I could not give you any informed answer to your question based on our interaction with the intelligence/counterintelligence. But I would also defer to the second panel where the director of the counterintelligence is going to be a witness.

Mr. INSLEE. Well, I would ask the panel to take a look at it and provide us your review, if you can do so. I do think it brings up some significant issues which would suggest there has been a real

change of emphasis, and we would appreciate your further comments. Thank you.

I yield back.

Mr. STUPAK. The gentleman yields back. Let me thank and ask this panel—that's all the questions we are going to ask you in open session; as you referred to once or twice, we will go to closed session after the next panel. So I would ask that you just stay in the vicinity, not necessarily have to sit in the hearing room because we are going to do the next panel which has eight witnesses. It will take us some time, but we are going to go into closed session. We will invite you back for closed session. Thank you.

I am going to ask our next panel to come forward, please.

On our second panel we have Dr. Michael Anastasio, the Director of the Los Alamos National Laboratory; Dr. George Miller, who is the Director of Lawrence Livermore Laboratory; Dr. Thomas Hunter, who is the President and Laboratory Director at Sandia National Laboratories; Mr. Thomas Pyke, Jr., who is the Chief Information Officer at the Department of Energy; Dr. Linda Wilbanks, who is the CIO, Chief Information Officer, at the National Nuclear Security Administration within the Department of Energy; Mr. Bradley Peterson, who is the Chief and Associate Administer for the Defense Nuclear Security at the National Nuclear Security Administration within the Department of Energy; and Mr. Stanley Borgia, who is the Deputy Director for Counterintelligence in the Office of Intelligence and Counterintelligence at the Department of Energy.

Have we got everybody? We are missing Dr. Wilbanks. We will have to wait for Dr. Wilbanks here for a minute. It will be just a second. And it looks like Mr. Peterson, too.

[Brief recess.]

Mr. STUPAK. It is the policy of this subcommittee to take all testimony under oath. Please be advised that witnesses have the right under the rules of the House to be advised by counsel. Do any of you wish to be advised by counsel? Everyone shook their head no. So we will do the oath.

Do you swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth in the matter pending before this subcommittee?

[Witnesses sworn.]

Mr. STUPAK. Let the record reflect all of our witnesses took the oath. You are now under oath. We will start with 5-minute opening statements.

I understand, Mr. Peterson, you wish to go first. So we will accommodate that request for your opening statement, please.

STATEMENT OF BRADLEY A. PETERSON, CHIEF AND ASSOCIATE ADMINISTRATOR, DEFENSE NUCLEAR SECURITY, NATIONAL NUCLEAR SECURITY ADMINISTRATION

Mr. PETERSON. Good morning, Chairman Stupak, Ranking Member Shimkus, members of the subcommittee. My name is Brad Peterson. I was recently appointed Chief Defense Nuclear for the National Security Administration, the NNSA. Prior to this appointment, I was the Director of the Office of Independent Oversight within DOE's Office of Health Safety and Security. It gives me a

unique perspective into the issues to be discussed today. In my new role, I have overall responsibility for physical and cybersecurity within NNSA.

Following my remarks, Dr. Linda Wilbanks, the NNSA Chief Information Officer with operational responsibility for cybersecurity, will provide her opening comments.

While the NNSA faces many challenges and it has significant room to improve, we continue to make enhancements in our physical and cybersecurity postures to maintain strong and robust security. NNSA operates some of the most secure facilities in the world and generally maintains effective physical security programs. Over the last 2 years, while there have been some issues, we see overall progress in improving performance at the NNSA weapons laboratories.

Earlier this year, the Office of Independent Oversight conducted a safeguard security inspection of Lawrence Livermore National Laboratory and identified significant weaknesses in protective force operations, based in part on poor performance during force-on-force training exercises.

Immediately after the inspection results were known, the Office of Defense Nuclear Security within NNSA devoted considerable attention to understanding the issues and providing subject matter expertise from across NNSA. While the NNSA was not pleased with their results from the Livermore inspection, I can attest to the fact that the Office of Defense Nuclear Security Livermore site office and laboratory have taken the issues very seriously and worked aggressively to implement corrective actions.

Livermore launched a comprehensive recovery plan, and today we see the results of their efforts taking hold. Protection force capability at Livermore is much improved and there are more changes in progress.

Upon assuming my new position in June, the NNSA Administrator directed me to dispatch a team of senior NNSA security professionals to conduct an onsite review of the Los Alamos National Laboratory Protective Force operation to determine if they had similar issues. The NNSA team found that the Los Alamos Protective Force had a strong and rigorous performance testing program and was performing effectively. This assessment of Los Alamos was reinforced by preliminary positive results from the recently completed independent oversight inspection.

Seeking to build sustainable security programs, I intend to look across the NNSA for examples of where we are getting it right. We are also engaging in efforts to improve the flow of information across the NNSA security community through our security leadership coalition. The coalition has been actively engaged in evaluating the underlying causes of security and management issues that we face and developing standardized solutions. The objective of this effort is to break down organizational stovepipes and turn a previously reactive approach to security problems into a proactive approach.

NNSA is making real and fundamental changes to our security program. These changes seek to reduce the opportunity for human error by relying on engineered controls. We are also focused on making our security challenges easier by reducing our classified

footprint. We have emphasized the need for strong contractor assurance programs designed to spot problem areas quickly and resolve them before they turn into real security issues.

Finally, we need to continue to develop a strong Federal security staff that is technically capable. We need to ensure that our Federal oversight program takes advantage of the tools at our disposal, including substantial deductions of award fee for poor performance and fines provided under 10 CFR 824 when appropriate. We also need to ensure that we are appropriately incentivizing and rewarding the right behaviors to drive needed improvements.

In closing, since taking over as the Chief Defense Nuclear Security, I have seen a renewed sense of commitment across the NNSA security community to improve performance through the sharing of lessons learned and working collectively to address significant challenges. Security activities at our national labs are large and complex. The security professionals within NNSA are working together today to reduce the opportunities for error and react quickly to any problems that do occur.

Mr. PETERSON. I am confident in our ability to continue to grow and I look forward to the continued challenge.

That concludes my opening comments. I would be pleased to answer any questions after other opening statements.

Mr. STUPAK. Thank you, Mr. Peterson.

[The prepared statement of Mr. Peterson follows:]

Testimony Highlights

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

- While the NNSA faces many challenges, and has room to improve, we continue to make enhancements in our physical and cyber security posture that will maintain security at our sites as strong and robust.

- Whether it is the physical or the cyber threat, the first premise on how we protect our most important information is based upon the government-wide processes for the protection of multiple levels of classified information, material and technologies and the application of risk management principles. We utilize a graded security approach, with defense in depth security systems, based on the information and assets at each facility or on each network, and the perceived threat to that facility. Our security is continuously tested and evaluated to expose weak links and areas for improvement.

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

- NNSA operates some of the most physically secure facilities in the world and generally have maintained effective programs and seen positive improvements in the past two years in the area of physical security at the weapons' laboratories. That said, we face many challenges in consistently maintaining fully effective programs. An exhaustive security planning process, a detailed program development process, and in-depth controls and oversight of the implementation of our programs provide the basis for ensuring security readiness.

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

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

September 25, 2008

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

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

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

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

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

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

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

The Cyber Security Challenge

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Physical Security Challenge

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

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

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

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

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

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

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

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

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

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

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

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

- Completing the removal of Category I and II Special Nuclear Material from Sandia National Laboratory-New Mexico and re-distributing armored vehicles, weaponry, and ammunition to other sites in the Complex.

- Progressing ahead of schedule, and utilizing all available shipping capacity, to eliminate Category I and II Special Nuclear Material from LLNL by 2012.

- Adding additional barriers and weapons systems, and enhancing nuclear material vaults.

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

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

- Reducing our classified footprint at sites like LANL.

Not withstanding these improvements, both DOE and GAO auditors have highlighted areas at LANL where we must devote additional attention and resources. The GAO in particular is concerned with our ability to sustain the improvements made at LANL and identified the need for us to have a better strategic plan. Given the history at Los Alamos it is hard to disagree with those concerns and the recommendation. We have recently hired a new Federal security manager for the site and my office will be working closely with him and his staff to build a strong security program at Los Alamos and address these issues. As the GAO and DOE auditors point out – there is a strong foundation of improvements to build from, the key of course is sustainment of the security improvements, this will continue to be a primary objective for NNSA in the coming years.

Summary

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

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

Mr. STUPAK. Mr. Pyke, let's start with you. We'll go right down the line. And your opening statement, please, for 5 minutes. If you have a longer statement, it will be submitted for the record.

STATEMENT OF THOMAS N. PYKE, JR., CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

Mr. PYKE. Good afternoon, Chairman Stupak, Ranking Member Shimkus, members of the subcommittee. My name is Tom Pyke. I am Chief Information Officer of the Department of Energy.

Over the past 3 years the Department has undertaken a major effort to improve its cyber security posture. DOE has a comprehensive cyber security program that includes establishment of DOE-wide policy, a senior-level governance structure, cyber security awareness and specialized cyber security training, improved cyber security incident management and compliance monitoring.

The program is governed according to a cyber security management order issued in December 2006. This order directs the use of a risk-based approach to cyber security management, and it establishes a governance structure within the Department that assigns primary responsibility for implementation of cyber security to the Under Secretary and other senior leaders. These senior leaders determine and assess program-unique threats and risks and they issue direction for implementing cyber security within their respective organizations.

DOE-wide cyber security direction, including direction for special protection of sensitive unclassified information, builds on government-wide guidance from the Office of Management and Budget as well as Federal information processing standards and other cyber security guidance issued by the National Institute of Standards and Technology. We also follow applicable guidance issued by the Department of Defense.

Employing a risk-based approach, DOE senior management, including NNSA, has given special attention during the past year to the graded protection of DOE systems and data, taking into account threat and risk and the sensitivity of the data. Under our cyber security governance structure, each part of the Department reviews the sensitivity of the data under its jurisdiction relative to the strength of the controls that are in place to protect the data and takes action to strengthen those controls if needed.

The management of cyber security incidents is an integral part of cyber security management, including providing timely alerts to the entire Department of known threats, detecting cyber attacks as they occur or as soon as possible afterward and responding to such attacks. The response includes reporting all cyber security incidents to the US-CERT, which is the Federal Government's cyber incident handling center. It also includes mitigating the potential adverse impact of each incident at the site at which it was detected and elsewhere in the complex, determining the impact of the incident and repairing any damage or disruption resulting from the incident.

Cyber attacks are increasing in complexity and frequency and are becoming more aggressive. DOE is attacked over 10 million times each day in a wide variety of ways, and DOE has in-depth protection mechanisms in place throughout the complex. Even with

this protection, some of the most sophisticated attacks against DOE have, on occasion, been able to penetrate our unclassified systems and networks.

DOE has an in-depth cyber security defense based on industry and government best practices. And we continually improve our defenses, including our ability to detect attacks. However, some cyber attacks continue to evolve to avoid detection by these defenses.

Within the Department, the Office of the Chief Information Officer and NNSA cooperate in the reporting of cyber incidents and support tour sites as they handle each incident. The Office of the CIO and NNSA have recently signed an agreement to improve further the way we work together to respond to cyber incidents. Our office also works in partnership with the Department's Office of Intelligence and Counterintelligence as we prepare for future cyber attacks and respond to them. Counterintelligence data analysis associated with activities that may have a foreign nexus provides useful input to the cyber security incident management process led by the Office of the CIO.

I would be pleased to respond to any questions you may have, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Pyke.

[The prepared statement of Mr. Pyke follows:]

TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

September 25, 2008

- The Office of the Chief Information Officer has primary responsibility for cyber security within the Department of Energy. Over the last three years, the Department has undertaken a major effort to improve its cyber security posture.

- DOE has a comprehensive cyber security program that includes establishment of DOE-wide policy, a senior level governance structure, cyber security awareness and specialized cyber security training, improved cyber security incident management, and compliance monitoring.

- DOE has issued a Cyber Security Management Order, a National Security Systems Manual, a Cyber Security Process Requirements Manual, and 18 cyber security "technical and management requirements" documents.

- DOE employs a risk-based approach to cyber security management that places primary responsibility for implementation of cyber security on the Under Secretaries, including the Under Secretary for Nuclear Security, who is the Administrator, National Nuclear Security Administration, and other key leaders.

- Cyber attacks are increasing in complexity and frequency, and are becoming more aggressive. DOE is attacked over ten million times each day in a wide variety of ways, although DOE has defense-in-depth mechanisms in place throughout the complex.

- The management of cyber security incidents is an integral part of cyber security management, including providing timely alerts to the entire Department of known threats, detecting cyber attacks as they occur or as soon as possible afterward, and responding to such attacks.

- The Office of the Chief Information Officer works in partnership with the Department's Office of Intelligence and Counter Intelligence as we prepare for future cyber attacks and respond to them.

TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

September 25, 2008

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. The Office of the Chief Information Officer has responsibility for cyber security within the Department.

Over the last three years, the Department has undertaken a major effort to improve its cyber security posture. DOE has a comprehensive cyber security program that includes establishment of DOE-wide policy, a senior level governance structure, cyber security awareness and specialized cyber security training, improved cyber security incident management, and compliance monitoring.

The program is governed according to a Cyber Security Management Order that was issued in December 2006. This Order directs the use of a risk-based approach to cyber security management, and it establishes a governance structure within the Department that places primary responsibility for implementation of cyber security on the Under Secretaries, including the Under Secretary for Nuclear Security, who is the Administrator, National Nuclear Security Administration (NNSA), and other key leaders. These senior leaders determine and assess program-unique threats and risks, and they issue direction for implementing cyber security within their respective organizations.

In addition to the cyber security management order, we have issued a National Security Systems Manual, a Cyber Security Process Requirements Manual, and 18 cyber security "technical and management requirements" documents. This DOE-wide cyber

security direction builds on government-wide guidance from the Office of Management and Budget and Federal Information Processing Standards and other cyber security guidance issued by the National Institute of Standards and Technology, as well as applicable guidance issued by the Department of Defense. The Under Secretaries, the Administrator of the Energy Information Administration, the Power Marketing Administrations, and I have developed Program Cyber Security Plans that apply these DOE requirements as well as government-wide requirements within each of our DOE organizations.

Employing the risk-based approach, DOE senior management, including NNSA, has given special attention during the past year to the graded protection of DOE systems and data, taking into account threat and risk and the sensitivity of the data. As a part of this effort, it is appropriate for each part of the Department to review the sensitivity of the data under its jurisdiction relative to the strength of the controls that are in place to protect that data, and to strengthen those controls if needed after such a review.

The management of cyber security incidents is an integral part of cyber security management, including providing timely alerts to the entire Department of known threats, detecting cyber attacks as they occur or as soon as possible afterward, and responding to such attacks. The response includes reporting all cyber security incidents to the US-CERT, the Federal government's cyber incident handling center. It also includes mitigating the potential adverse impact of the incident, at the site at which it was detected and elsewhere in the DOE complex, determining the impact of the incident, and repairing any damage or disruption resulting from the incident.

DOE assists other agencies and receives information that helps DOE to defend its systems through participation in the interagency cyber security information sharing activities operated by the DOD Joint Task Force-Global Network Operations and other

organizations. We participate in the planning for and expect to benefit from planned activities of the government-wide Comprehensive National Cybersecurity Initiative.

Cyber attacks are increasing in complexity and frequency, and are becoming more aggressive. DOE is attacked over ten million times each day in a wide variety of ways, and DOE has defense-in-depth mechanisms in place throughout the complex. Even with this protection, some of the very sophisticated attacks on DOE have, on occasion, been able to penetrate our unclassified systems and networks. DOE has a cyber security defense based on industry and government best practices, and we continually improve our defenses, including our ability to detect attacks. However, some cyber attacks continue to evolve to avoid detection by these defenses.

Within the Department, the Office of the Chief Information Officer and NNSA cooperate in the reporting of cyber incidents and support to our sites as they handle cyber incidents. The Office of the CIO and NNSA have recently signed an agreement to improve further the way we work together to respond to cyber incidents. Our Office works in partnership with the Department's Office of Intelligence and Counterintelligence as we prepare for future cyber attacks and respond to them. Counterintelligence data analysis associated with activities that may have a foreign nexus provides useful input to the cyber security incident management process led by the Office of the CIO.

I would be pleased to respond to any questions you may have.

Mr. STUPAK. Dr. Wilbanks, your opening statement, please.

STATEMENT OF LINDA R. WILBANKS, PH.D., CHIEF INFORMATION OFFICER, NATIONAL NUCLEAR SECURITY ADMINISTRATION, U.S. DEPARTMENT OF ENERGY

Ms. WILBANKS. Chairman Stupak and members of the subcommittee, I am Dr. Linda Wilbanks, Chief Information Officer for the National Nuclear Security Administration. Thank you for the opportunity to appear before you today regarding the NNSA's cyber security program. As the CIO, I am responsible to ensure the protection of electronic classified and unclassified information.

The cyber threats to the Department of Energy and NNSA are similar to those faced by the Federal Government, every public and private enterprise, and every individual. NNSA's facilities are targeted, over 1 million cyber attacks every day of varying sophistication, ranging from relatively harmless curiosity seekers to sophisticated hackers to corporate thieves and national state and belief-based espionage.

In response to these threats, NNSA has established a robust technical operational managerial-based approach to cyber security of unclassified, controlled unclassified and classified information. We believe our approach, which is continually improving, is sound and provides effective security for our unclassified and classified networks.

Even with a wide range of threats, I can say very confidently that our classified networks, which protect our crown jewels are extremely well protected. We operate separate networks for our classified information, which are air-gapped from our unclassified networks. We've implemented a diskless workstation initiative across the complex to manage the movement of data within the classified networks.

We also have a wide range of technical and administrative controls to manage access to the data that resides on our controlled unclassified networks, which, while not classified, may include important information. This information requires added protection, including encryption during transmission and at rest, the use of two-factor authentication for remote access.

We continue to assess other controls, collaborating with our peers in government, leveraging the results of the assessments to find even better ways to protect our unclassified networks. Other defense and depth tools we use for cyber protection are multiple firewalls and monitoring systems to check for incoming, outgoing and internal unclassified network traffic to ensure it is authorized and there are no anomalies.

When our systems detect unusual activities, we quickly terminate the communication pathways, and when necessary, selectively isolate portions of our network to quarantine any potentially harmful activities. Once a harmful activity is isolated, we deploy our exceptional forensics capabilities to eradicate the threat, restore the systems to secure operations.

Policy and standards are an important part of establishing an effective cyber security program, and in May 2008 NNSA's cyber security policy was issued, addressing many previous recommendations and findings. This policy was developed in collaboration with

our sites, incorporates the recently issued DOE National Security Manual and many of their requirements, such as security plans and certification and accreditation procedures have already been implemented.

We also have established strong and effective cyber security incident response capabilities. The DOE and NNSA have partnered to implement a state-of-the-art facility in Las Vegas, Nevada. This facility monitors DOE and NNSA networks and coordinates the response to incidents by utilizing extensive communications and collaboration among DOE/NNSA sites, other Federal agencies, law enforcements, intelligence, and counterintelligence.

In summary, NNSA has a robust technical, operational and management-based approach to cyber security of the unclassified, the controlled unclassified and the classified information. However, we acknowledge the need for continual improvement. We believe our approach is fundamentally sound, but the nature of the threat changes daily. We must keep pace with the adversary and continue to improve the collaboration between our sites, DOE counterintelligence and the cyber security experts across the government and industry to succeed in the future.

This concludes my opening statement. And I'm pleased to answer questions at the end.

Mr. STUPAK. Thank you.

[The statement of Ms. Wilbanks is included with the statement of Mr. Peterson.]

Mr. Borgia, your opening statement, please.

STATEMENT OF STANLEY J. BORGIA, DEPUTY DIRECTOR FOR COUNTERINTELLIGENCE, OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, U.S. DEPARTMENT OF ENERGY

Mr. BORGIA. Thank you, Mr. Chairman.

Mr. STUPAK. You may want to pull that a little closer. It doesn't pick up very well.

Mr. BORGIA. Chairman Stupak, Ranking Member Shimkus and distinguished members of the committee, thank you for the invitation to appear before you on a subject of importance, the cyber threat.

I'm addressing you today as the Deputy Director of Counterintelligence in the Department of Energy's Office of Intelligence and Counterintelligence. However, sir, I would like to go just a little further in my introduction, because there is a letter that is controversial, and explain to you that I am also a Deputy Assistant Director in the FBI, assigned by Director Mueller to the Secretary of Energy to run the counterintelligence program. I have been here for over 2 years, since July of 2006, and I will continue.

We and DOE counterintelligence are both a producer of intelligence information and a consumer of intelligence information. We develop and facilitate the transfer of DOE-unique information to the United States Intelligence Community and convey actionable Intelligence Community threat information to all departmental action offices, including the National Nuclear Security Administration, NNSA. We appreciate that physical security is an essential element in the protection of information, and we participate in the

National Joint Terrorism Task Force, National Counterterrorism Center, to enhance the protection of DOE equities.

Likewise, we are a very active member of the FBI-led National Cyber Investigative Joint Task Force, or NCIJTF, which allows us to provide unique DOE and NNSA information to the cyber investigations community and collaborate at national initiatives. Membership also provides DOE with invaluable current cyber-based threat information relevant to our departmental assets and critical energy infrastructure.

DOE's Counterintelligence Office performs a broad range of cyber-related functions, including analysis of cyber security incidents with a foreign nexus. Our work is closely coordinated with the DOE Office of the Chief Information Officer and the NNSA's Office of the Chief Information Officer with which we've maintained a strong and mutually supportive relationship in the cyber security team.

The nature of the cyber threat to the DOE complex is constantly evolving. DOE sensors, monitoring attacks on the DOE networks, have picked up an increased tempo of potential adversarial activity, including network reconnaissance, scanning for potential attack vectors and outright cyber attacks. In 3 of the past 6 months sensors have documented well over 400 million such indicators of hostile activity every month.

Further, we have seen thousands of socially engineered e-mails. They may appear to come from known associates or support an interesting subject line, but they contain malicious computer code designed to infect the recipient's computer, steal and transmit information it contains, and eventually spread to the rest of the network. A single mouse click by a single user can contaminate large numbers of networked computers.

In order to generate counterintelligence investigative leads from all this activity, I have directed expanded use of cyber techniques at DOE and NNSA. The results have been dramatic. In particular, cyber tools developed under this initiative have enabled investigators at the intelligence and military organizations to make strides toward attribution for ongoing computer intrusions directed against DOE and other United States Government computer networks, a major accomplishment for DOE, that has demonstrated the value of these cyber tools for CI analysis.

The counterintelligence cyber program has developed professional working relationships with the Defense Information Systems Agency, the Military Service Information Operation Centers, the military service Criminal Investigation Divisions and the Joint Information Operations Warfare Analysis Center in San Antonio, Texas. These are comprehensive information-sharing relationships as well as expanded partnerships for information and cyber data exchange. They serve to increase awareness of the operational methods being employed by individuals and state-sponsored entities engaged in unauthorized computer intrusions into DOE computer networks.

DOE in collaboration with the Intelligence Community partners, DOE national laboratories, chief information officers and DOE cyber security use data integration tools and intrusion detection

sensors to uncover, investigate and mitigate suspicious cyber events with a foreign nexus.

In closing, Mr. Chairman, the attacks we see place virtually every computer connected to the Internet at risk of compromise, including those of the U.S. Government and our critical energy infrastructure. Moreover, an attacker has a significant advantage over the protect-and-defend cyber security community. DOE's Office of Intelligence and Counterintelligence will continue to pursue all available lawful means to detect, investigate and mitigate the pervasive cyber threats we as a nation now face.

Thank you, Mr. Chairman.

Mr. STUPAK. Thank you.

[The prepared statement of Mr. Borgia follows:]

TESTIMONY OF
STANLEY BORGIA
ASSOCIATE DIRECTOR OF COUNTERINTELLIGENCE
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE OF ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

September 25, 2008

Chairman Bart Stupak, Ranking Member John Shimkus, and distinguished members of the committee, thank you for the invitation to appear before you on a subject of critical importance: "The Cyber Threat." I am addressing you today as the Deputy Director, Counterintelligence, in the Department of Energy's (DOE) Office of Intelligence and Counterintelligence.

We in DOE Counterintelligence are both a producer of intelligence information, and a consumer of intelligence information. We develop and facilitate the transfer of DOE-unique information to the United States Intelligence Community, and convey actionable Intelligence Community threat information to all Departmental action offices, including NNSA.

We appreciate that physical security is an essential element in the protection of information, and we participate in the National Joint Terrorism Task Force/National Counter Terrorism Center to enhance the protection of DOE equities.

Likewise, we are a very active member of the FBI-led National Cyber Intrusion Joint Task Force, or NCIJTF, which allows us to provide unique DOE and NNSA information to the cyber investigations community and collaborate in national initiatives. Membership also provides DOE with invaluable current, cyber-based threat information relevant to our own Departmental assets and critical energy infrastructure.

DOE's counterintelligence office performs a broad range of cyber-related functions, including analysis of cyber security incidents with a foreign nexus. Our work is closely coordinated with DOE's Office of the Chief Information Officer (OCIO) and with NNSA's Office of the Chief Information Officer (OCIO), with which we maintain a strong and mutually supportive relationship in the cyber security realm.

The nature of the cyber threat to the DOE complex is constantly evolving. DOE sensors monitoring attacks on the DOE networks have picked up an increased tempo of potential adversarial activity, including network reconnaissance, scanning for potential attack vectors, and outright cyber attacks. In three of the past six months, sensors have documented well over 400 million such indicators of hostile activity every month. Further, we have recently seen thousands of socially engineered e-mails. They may appear to come from known associates or sport an interesting subject line, but they contain malicious computer code designed to infect the recipient's computer, steal and transmit information it contains, and eventually spread to the rest of the network. A single mouse click by a single user can contaminate large numbers of networked computers.

In order to generate counterintelligence investigative leads from all this activity, I have directed expanded use of cyber techniques at DOE and NNSA. The results have been dramatic. In particular, cyber tools developed under this initiative have enabled investigators at intelligence and military organizations to make strides toward attribution for ongoing computer intrusions directed against DOE and other United States Government computer networks—a major accomplishment for DOE that has demonstrated the value of these cyber tools for CI analysis.

The Counterintelligence Cyber Program has developed professional working relationships with the Defense Information Systems Agency, the military service Information Operations Centers, the military service Criminal Investigation Divisions, and the Joint Information Operations Warfare Analysis Center in San Antonio, Texas. These are comprehensive information sharing relationships, as well as expanded partnerships for information and cyber data exchange. They serve to increase awareness of the operational methods being employed by individuals and state sponsored entities engaged in unauthorized computer intrusions into DOE computer networks. DOE—in collaboration with the Intelligence Community partners, DOE National Laboratories, Chief Information Officers and DOE Cyber Security—use data integration tools and intrusion detection sensors, to uncover, investigate, and mitigate suspicious cyber events with a foreign nexus.

In closing, the attacks we see place virtually every computer connected to the Internet at risk of compromise, including those of the U.S. Government and our critical energy infrastructure. Moreover, an attacker has a significant advantage over the "protect and defend" cyber security community. DOE's Office of Intelligence and Counterintelligence will continue to pursue all available lawful means to detect, investigate, and mitigate the pervasive cyber threats we, as a nation, now face.

This concludes my testimony and I look forward to answering any questions you may have.

Mr. STUPAK. Dr. Anastasio, please, for your opening.

STATEMENT OF MICHAEL R. ANASTASIO, PH.D., DIRECTOR, LOS ALAMOS NATIONAL LABORATORY

Mr. ANASTASIO. Thank you, Mr. Chairman and Ranking Member Shimkus. I'm Dr. Michael Anastasio, Director of the Los Alamos National Laboratory. Thank you for the opportunity to discuss the lab's continuing efforts to improve and sustain security.

For my first appearance before this subcommittee in January of 2007, I clearly understood the message from the Members: Continued security issues at Los Alamos were not going to be tolerated. I'm pleased to report that at Los Alamos we now have a record of successes in both physical security and cyber security. We've taken concrete actions to reduce risk, clarify policy, establish roles and responsibilities and develop solutions to continuously improve the security posture at our site.

These measures are working. Over the past year the laboratory has reduced potential unauthorized disclosures of information by two-thirds, and that number continues to improve.

My written statement details our progress, but there are three points I'd like to make here now. First, I am especially proud that the improvements made at the laboratory link directly to the actions and attitudes of our employees. Members of our workforce have very little tolerance for any of their coworkers who are not security conscience. The workforce understands that the Nation must trust them to handle our most sensitive secrets, and our actions have helped justify that trust.

Second, the changes by the employees of Los Alamos have been coupled with an aggressive security improvement program. For example, we've reduced the number of vault-type rooms by one-quarter. We've reduced our classified accountable, removable electronic media from 12,000 items to fewer than 4,000. We've designed and opened the first supervault-type rooms and are planning for more. We've converted 94 percent of our targeted classified workstations to diskless operation. We've destroyed more than 40,000 classified nuclear weapon parts and more than 3 million pages of classified documents.

We're implementing a further segregation of our unclassified cyber network that will provide foreign national employees access only to the information that they require for their jobs.

And, third, in anticipation of how the cyber threat will continue to evolve, we're developing new approaches and technologies so that we can get ahead of the game to better protect our unclassified networks.

I'm encouraged that the three recent assessments in the testimony we heard on the previous panel by our external reviewers from GAO and HSS have validated our significant progress. However, these reports also clearly demonstrate that we need to make further improvements. I agree, and we're moving aggressively to address them.

Continuous security improvement is essential, and nowhere is this more evident than in cyber security. As I expressed in my last appearance before you, the cyber threat remains my most great concern. This is an ever-increasing, evolving threat from adver-

saries who are relentless and technically skilled. Protecting our classified resources is my highest priority, but further securing our unclassified yellow network is essential.

This network is the backbone of our operation. It's crucial that we develop solutions that manage risk and allow users to access the information they need to do their jobs. One example is something we call "glove box computing." With this technology, a user can access, create and manipulate information, but has no ability to remove it, similar to how we handle nuclear material.

The cyber threat is one faced by the entire Nation. It's something that requires a coordinated national response using our country's combined assets, skills and experience. The unique cyber capabilities of the national laboratories can be a valuable resource, building on the integration efforts that are already under way among all three of our laboratories and with NNSA and DOE.

In conclusion, Mr. Chairman, Los Alamos is making significant progress improving our security posture, and we are committed to continuous improvement to stay ahead of the evolving threat. I would like to invite you and other members of the committee to come visit the lab and see how we're doing.

And with that, I'll thank you and be ready to take your questions.

[The prepared statement of Mr. Anastasio follows:]

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.

Mr. STUPAK. Well, thank you. And I know the staff was just there, and unfortunately they didn't get a chance to meet with you. But hopefully there will be another time, and hopefully it's not when we're there looking at a lapse or something.

But I think we all know that there have been improvements at Los Alamos.

Mr. ANASTASIO. Thank you. I appreciate that.

Mr. STUPAK. Dr. Miller, your opening statement, please.

STATEMENT OF GEORGE H. MILLER, PH.D., DIRECTOR, LAWRENCE LIVERMORE NATIONAL LAB

Dr. MILLER. Mr. Chairman, members of the committee, thank you for the opportunity to provide you my perspective on the security challenges we face together.

As the director of a national security laboratory, I am very familiar with the threats to our Nation and take very seriously our special responsibilities to protect special nuclear materials and some of the Nation's most sensitive secrets. Safety and security are my highest priorities, and they are integrated into a single culture at the laboratory.

Particularly in the cyber security area, threats are rapidly evolving, continue to grow more sophisticated. My approach involves anticipation, prevention, detection, response and sustainment through continuous improvement.

The laboratory uses a variety of techniques to assess both physical and cyber security, and they are an integral part of our continuous improvement efforts. These include GAO audits, ongoing site inspections by DOE's Office of Health Safety and Security, local site surveys and our own self-assessments.

The HSS inspection this last spring was instrumental in helping us identify deficiencies in our security readiness. In summary, the HSS, as you have heard, found significant weaknesses in two areas, protective force and classified matter protection. We've made significant progress in addressing these inspection findings.

I led a thorough review of our actions and decisions to identify the root cause of what was an unacceptable decline in our protective force's level of posture demonstrated just 16 months earlier. I'm pleased to report that these actions have significantly improved the readiness of our protective force as demonstrated through a security incident response of a fully integrated force-on-force with an external adversary just 8 weeks ago. This exercise was monitored both by NNSA and HSS, and the Office of the Chief of Defense Nuclear Security concluded that the lab's effort has resulted in a posture of robust protection. Let me tell you how we achieved this.

In short, our analysis revealed that restrictions on and postponement of comprehensive robust exercises due to safety considerations had a detrimental effect on the protective force readiness. We have addressed those safety issues and resumed frequent exercises while ensuring the safety of our employees. My written testimony details some of these corrective actions. I'm committed to sustaining that performance and that level of progress, and we have scheduled future robust exercises quarterly to ensure that.

I believe that maintaining adequate cyber security requires constant attention, utilizing counterintelligence experts and informa-

tion technology professionals to anticipate, develop and deploy effective defensive systems and quickly respond to emerging threats to assure appropriate protection.

Over the last 2 decades Livermore has hosted and staffed the Department of Energy's computer incident advisory capability. This staff of highly trained computer scientists have provided support for the entire complex with forward-looking cyber analysis assessments, best practices and training. In this regard, HSS concluded that the lab faces significant challenges in this area, but has the teams, technologies and methods needed for success to effectively deliver and address cyber security.

Protecting classified information from compromise is my highest priority. That's why our classified network is air-gapped from the rest of the laboratory.

We also maintain a separate unclassified network to handle our unclassified and our business information. Within this yellow network, different functions are segregated and isolated. It is used for programmatic activities that are essential for the laboratory.

These functions require external communication. It is, therefore, connected to the Internet. But it is protected by a firewall. And again, as I said, within that network it is segregated—different functions are segregated. Constant daily vigilance is required to protect the network, and we use a comprehensive site-wide risk assessment methodology along with shared information from my colleagues at the other laboratories and across the Federal Government to focus our cyber security efforts on emerging threats.

As an element of our continuous improvement, the lab has developed a blue network to provide appropriate computer access for essential mission work by the lab's foreign nationals and our external collaborators. Technical controls separate that from the yellow network.

As another example of our continuous improvement and further segmentation of important data, last year I invested in the building of and the commissioning of a consolidated data center for unclassified data. This provides uniform physical protection, appropriate backup, enhanced reliability and, most important, state-of-the-art cyber protection.

In conclusion, Mr. Chairman, taking personal and collective responsibility for safety and security is a fundamental value of the laboratory and an expectation of all employees. I can assure you that I am committed to provide the security that you and your colleagues expect from Lawrence Livermore Laboratory.

I appreciate the opportunity to testify and welcome your questions.

Mr. STUPAK. Thank you, Dr. Miller.

[The prepared statement of Dr. Miller follows:]

STATEMENT OF GEORGE H. MILLER

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 multilayered, 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 sitewide 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.

Mr. STUPAK. Dr. Hunter, your opening statement, please, sir.

Dr. HUNTER. Thank you, Mr. Chairman.

Mr. STUPAK. You're going to need the mic there. Thanks.

STATEMENT OF THOMAS O. HUNTER, PH.D., PRESIDENT AND LABORATORIES DIRECTOR, SANDIA NATIONAL LABORATORIES

Dr. HUNTER. Thank you, Mr. Chairman, Ranking Member and distinguished members of the committee. I am Tom Hunter, President of Sandia Corporation and Director of Sandia National Laboratories. It's a pleasure to appear before you and talk about this extremely important matter.

Sandia, as you know, is a national security laboratory and part of the NNSA; and we develop and support the nonnuclear parts of the nuclear term, but we also are, further, involved in research and development across a wide range of national security areas. I provided written testimony at some length, but I would like to emphasize just a few points.

First, I would like to talk about our commitment and my personal commitment to security.

We can only serve the Nation in so many sensitive areas, and we do place security at the very top of our value system. I should also be clear that I do not support the view that science in our world and security should be in conflict or can be in conflict. I believe that science in the national interest must embrace effective security.

It is a matter of great personal pride that the Nation has entrusted us with this most sensitive information. I and my entire organization are committed to always honor that trust. We can all live up to our security responsibilities if we're ever vigilant and constantly aware of the threat facing us and any vulnerability that may occur. We have decades of experience evaluating the threats to our nuclear deterrent, and we've applied that experience to the cyber world as well.

The second point I would like to make is, this Nation's made a great investment in its classification system, both of information and materials. We see great value in that system and we use it as the foundation, the very core, of our security systems. And this allows us to place the most emphasis on our security systems in the right places where there's the most sensitivity.

We believe we have made great progress in the last few years in our protective systems for physical security. We've reduced our vulnerability to attack by limiting all discrete Category I and Category II nuclear material at our site. We did that just recently and ahead of schedule.

Last year we received the highest possible rating on all seven major areas of physical security in the evaluation done by DOE's

Office of Independent Oversight. Yet we do not believe, and it's my strong conviction, that we can rest on any of our accomplishments. The challenge will always be greater and our expectation will always be higher.

We're acutely aware of the threat of malicious insiders and have an active counterintelligence program and one that is acknowledged to be uniquely effective because of the strong integration we have because of counterintelligence and our cyber and physical security programs.

As the committee has so well noted, there is one area, though, that we, like the majority of the Nation's institutions, must be even more vigilant. We are part, and a fundamental part, of the Nation's cyber system. We find that modern information systems are essential to manage and operate an enterprise such as ours. But with this great enabler comes a great risk.

There have rarely been threats to the very core of our Nation's infrastructure as pervasive and as asymmetrical as a cyber threat. We have acted aggressively to address the cyber threat. We have three separate networks for cyber information. Each system has been uniquely designed for the security provisions of the information there. All are controlled and monitored centrally by the laboratory.

When I sign on to my personal computer, it reminds me every time, like every employee, that I will be subject to observation and should expect no privacy from our monitoring systems. We block over 80 percent of our incoming e-mail. We save and evaluate all cyber traffic at the laboratory by expert and electronic means. If any user on our system does not conform to our security requirements, we'll promptly terminate access from the system.

We maintain a complete registration of all devices on our system, deploy encryption for sensitive transmissions and require common operating environment for all desktops. Each network is subdivided into segments that have separate monitoring and separate need-to-know protection.

We have close ties with the other institutions in the Federal Government and the other laboratories in the DOE. When an attack occurs, there is a direct and effective communication between Sandia, other laboratories and the DOE.

Finally, I would like to close my comments with emphasis on one point that I think is most central to the path forward for the cyber-secure world of the future, and that's people. I've had the opportunity to witness the dedicated professionals who defend our cyber systems. I've come to admire and respect their talent, their expertise and their dedication. Each day—and in most cases, very long days—they face an adversary that is more creative and better equipped than the day before. And any day they may be called upon to scan enormous files and spot anomalies that could easily allude most trained observers. They may be called on to go to another laboratory to help sort out an ongoing attack.

Why do they do it? It is not a matter of compliance. It is not a matter of administrative requirement. It is not even a matter of compensation or reward. And it's certainly not because they could not work anyplace else. It is, in my judgment, because they are in-

dividually committed to serve this country, to defeat this pervasive threat.

I'm thankful each day they're there with us, and I believe they're examples of the country's principal hope in the coming escalation of cyber attacks—talented people surrounded by talented people and equipped with unique experiences and assets who devote their careers to this conflict. If we could do only one thing in the whole world of cyber security, it will be to apply our Nation's best minds to the problem, train them, hire them, support them, and empower them.

And I now urge the committee, with all of us, to do whatever we can to help create an environment where these people have the opportunity to commit, to excel and to prevail.

Thank you, Mr. Chairman; and I would be pleased to answer any questions.

Mr. STUPAK. Thank you, Dr. Hunter.

[The prepared statement of Dr. Hunter follows:]

Statement of Dr. Thomas O. Hunter
President, Sandia Corporation and
Director, Sandia National Laboratories

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
September 25, 2008

SUMMARY OF MAJOR POINTS

- Sandia has a longstanding culture of respect for security, rooted in a heritage of disciplined national service.
- The NNSA laboratories face a full spectrum of threats from multiple sources.
- The potential consequence of a terrorist organization obtaining a nuclear weapon or material is unacceptably high. We regard this prospect as the ultimate physical security threat. We regard the prospect of cyber attacks that have the potential to undermine the credibility of our nation's nuclear deterrent or that would allow a nation or other entity to develop a nuclear weapons capability as the ultimate cyber security threat.
- Sandia no longer possesses discrete Category I and II Special Nuclear Materials. These were eliminated by February 2008.
- Sandia was the first NNSA site to eliminate all discrete Category I and II Special Nuclear Materials, completing the project in February 2008, seven months ahead of schedule.
- Sandia controls and monitors all interactions between members of the Sandia workforce and foreign nationals.
- Sandia National Laboratories has three cyber environments, which are centrally managed and controlled.
- Sandia has taken many steps to improve cyber security in response to increased threats, providing an appropriate balance between protection and productivity..
- The balance of resources between physical security and cyber security has not yet been adequately adjusted to reflect the increased needs of cyber security.
- Sandia's experience in cyber security is a resource for DOE, its laboratories, and across many sites.
- In order to secure our cyber infrastructure, our nation must have a strong core of committed people with excellent skills supported with the necessary resources.

This page intentionally left blank.

Statement of Dr. Thomas O. Hunter
President, Sandia Corporation and
Director, Sandia National Laboratories

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
September 25, 2008

INTRODUCTION

Mr. Chairman and distinguished members of the Committee, thank you for the opportunity to testify. I am Tom Hunter, president of Sandia Corporation and director of Sandia National Laboratories. Sandia is a multiprogram national security laboratory owned by the United States Government and operated by Sandia Corporation[1] for the National Nuclear Security Administration (NNSA).

My statement describes security program management and performance at Sandia National Laboratories. I will also comment on how we are responding to security issues of concern both to us and to oversight entities. I will give special emphasis to the challenges of cyber security.

Security Management at Sandia National Laboratories

Sandia has a longstanding culture of respect for security, rooted in a heritage of disciplined national service. The leadership at Sandia National Laboratories regards security as a central responsibility in the execution of our missions.

Our security program begins at the top of our Integrated Laboratory Management System. Safeguards and Security is a primary policy area managed by laboratory leadership, with oversight by the Sandia Corporation Board of Directors. Top management has established an

[1] Sandia Corporation is a subsidiary of the Lockheed Martin Corporation under Department of Energy prime contract no. DE-AC04-94AL85000.

unambiguous policy framework for security that is deployed through our management system to every organizational unit of the laboratory.

The security program at Sandia is structured with clearly stated lines of authority, responsibility, and accountability. Sandia's chief security officer integrates security policies and practices across the functional areas of physical security, cyber and information security, export control, and counterintelligence. These functional areas are managed by seasoned professionals in those fields, supported by expert staff. Because security can only succeed if it engages the workforce as a whole, we strive to maintain security awareness among our people through an active program of training and education. As a result, we have an expectation that our people will understand and comply with security policies and requirements, and we have a culture in which security is regarded as imperative. At Sandia, self-reporting of security incidents carries no shame (the majority of incidents are self-reported), and security processes are accepted as integral to programmatic work.

Security at Sandia is structured on the concept of defense-in-depth, a strategy of layered defense that we employ for both physical and cyber security. It begins with classifying assets and information into categories and levels based on sensitivity and risk. The government-wide classification system provides the foundation for our approach to protecting assets. We then apply protection systems appropriate for each category and level. Secret information will have more layers of protection than unclassified controlled information, and top secret information will have additional layers of protection beyond secret. We apply the need-to-know principle to information sets in both secret and unclassified environments.

In the past few years, Sandia has achieved significant success in strengthening the security program and instituting management reforms aimed at enhancing asset protection levels. I am pleased to report that our progress has been noted in recent inspections by the Department of Energy (DOE). The "Independent Oversight Inspection of Safeguards and Security" of August 2007 identified all major areas as "effective performance." The fiscal year 2007 Performance Evaluation Report by NNSA stated, "Sandia significantly exceeded performance expectations in the area of safeguards and security." While these comments are gratifying, we always pursue continuous improvement, and we actively work to improve our security posture.

The key to a secure enterprise is constant vigilance and a continuous and deep understanding

of threats and vulnerabilities. We cannot withdraw from the modern way of conducting business and performing research, and yet we must balance our need for modern information systems and flexibility with the imperative for security. The nature of our work differs from that in industry and academia, and our security challenge is somewhat unique.

We Face a Full-Spectrum Threat

The NNSA laboratories face a full spectrum of threats from multiple sources. Theft, espionage, sabotage, the insider threat, and carelessness are longstanding areas of concern. The physical avenues of these threats continue to require strengthening and attention. But the expansion of computer and communications technology over the last decade or so has opened whole new avenues of attack that are formidable and challenging.

Sandia has been programmatically engaged for decades in the study of threats that affect our national missions. In the early 1970s, the predecessor to DOE tasked Sandia National Laboratories to address the issues surrounding the potential for theft and sabotage of nuclear materials at DOE facilities or in transit. About the same time, the U.S. Air Force initiated a program at Sandia for research and development leading to the deployment of physical security systems for protecting globally deployed critical assets. It was during this period that Sandia began to acquire technical capabilities in security modeling and analysis, security hardware, and security systems engineering.

Although the cyber challenge is comparatively recent, we have addressed antecedents to modern cyber security through our decades-long engagement in use-control systems for nuclear weapons. Today we gain extensive insights into the evolving cyber threat via our programmatic ties to other agencies with responsibilities in this arena, and through our own analysis of the attacks directed to us.

Multiple threats exist today, and therefore they must be assessed and prioritized. For the purposes of this Committee, let me simply articulate the highest level threat I see for physical security and for cyber security:

The potential consequence of a terrorist organization obtaining a nuclear weapon or nuclear materials is unacceptably high. We regard this prospect as the ultimate physical security threat we face, and we defend most vigorously against it in our physical security systems.

Multiple threats similarly exist in the cyber realm—attackers range from amateur hackers to nation-states. Potential consequences can range from agency embarrassment to disablement of critical national security control systems. Cyber attackers sponsored by nation-states are not limited by budget, resources, and regulations, and they enjoy an asymmetrical advantage over time. We regard the prospect of cyber attacks that have the potential to undermine the credibility of our nation's nuclear deterrent or that would allow a nation or other entity to develop a nuclear weapons capability as the ultimate cyber security threat. We defend against this prospect most vigorously.

We know that in both the physical and cyber arenas, an active insider would be an effective pathway for an adversary to accomplish its objective. Therefore, we place special emphasis on the integrity of our people and the role of counterintelligence as an integrated partner with our security programs.

Security Programs in Place at Sandia National Laboratories

Sandia manages its security operations in a systematic and disciplined way. We strive to comply with all applicable directives and requirements. We see compliance as the essential baseline—the platform from which we can advance our security performance.

Sandia's assurance system for security management and performance applies the elements of Sandia's Integrated Laboratory Management System at all Sandia sites. The Safeguards and Security Assurance Program provides management and oversight entities with an understanding of compliance and performance through analysis and trending of relevant data. We are working to enhance our trending capabilities by developing new metrics that provide more meaningful information. The key elements of the assurance system are self-assessments, performance assurance testing, and corrective action management. The assurance program helps management monitor the health of the security program, identify areas for improvement and design corrective actions, and ensure long-term sustainability.

Sandia's security program implements short, mid, and long-term strategies aligned with the laboratory's strategic plan and program guidance provided by the NNSA. The strategies are translated into prioritized goals with specific deliverables in our annual Safeguards and Security Implementation Plan, approved by DOE's Sandia Site Office and monitored quarterly by

NNSA's Defense Nuclear Security Office.

Physical Security

An important objective in our physical security program has been to reduce the inventory of special nuclear materials (SNM) at Sandia sites. NNSA Administrator D'Agostino set a goal to consolidate SNM at five NNSA sites by 2012. Sandia was the first NNSA site to eliminate all discrete Category I and II SNM, completing the project in February 2008, seven months ahead of schedule. Sandia no longer possesses SNM in quantities that require a threat level 1 protection. This inventory reduction has made it possible for us to implement cost savings in our security program.

In 2007 Sandia placed a cap on the total number of vault-type rooms (VTRs) that would be allowed to exist to support mission activities. We initiated a project to examine the mission and security needs for every existing VTR. This rejustification project required line managers to look for opportunities to reduce classified holdings and consolidate and reduce storage locations, consistent with mission needs. To date, the VTR re-justification project has resulted in a 16-percent reduction in the number of VTRs at our New Mexico site and an even greater reduction at our California site.

Sandia's chief security officer has established a Sandia Security Footprint Advisory Council composed of senior managers from organizations across the laboratory as well as representatives from our Facilities group. The council is advising management on ways to effectively manage Sandia's security footprint and associated risks while assuring robust security.

Sandia controls and monitors all interactions between members of the Sandia workforce and foreign nationals in a fashion that is commensurate to the risks involved. All substantive relationships between Sandians and foreign nationals, whether business or personal and regardless of where they occur, must be reported to Sandia's counterintelligence office. A security plan is prepared for each foreign national employed by or visiting Sandia that must document the specific physical and cyber access that is authorized. These security plans are reviewed by subject-matter experts from Sandia's physical security, cyber security, counterintelligence, export control, classification, and operational security organizations before approval by the appropriate Sandia vice president. Foreign nationals who are citizens of or were born in countries on the DOE sensitive country list are subject to special scrutiny. Any indication

of behavior beyond that which is authorized is a matter of special security and counterintelligence attention.

Access to classified information requires the appropriate level U.S. Government security clearance and a valid need-to-know. Access to export-controlled information is permitted only if a foreign national has legal permanent residency and a valid need-to-know. Access to other unclassified controlled information, including personal identity information, is also limited by need-to-know.

Employment as a regular Sandia employee is restricted by Sandia policy to individuals who are eligible for a U.S. Government security clearance, which generally means United States citizens. Exceptionally talented foreign nationals who are committed to becoming U.S. citizens may be hired as regular Sandia employees upon completion of a counterintelligence investigation.

The 2008 DOE inspection of Sandia's counterintelligence program lauded the excellent and mutually beneficial relations that exist at Sandia between counterintelligence and both cyber and physical security. The close involvement of counterintelligence with security is essential for strengthening protections against the insider threat.

Assurance is a crucial component of our security program because it engages line organizations directly in security improvement. Self-assessments, a key component of our assurance program, are completed on an annual schedule in accordance with requirements in the relevant DOE directives and are conducted with the assistance of qualified personnel. Self-assessment results are analyzed and trended in Quarterly Management Assurance Reports incorporated in Sandia's Integrated Laboratory Management System. A formal process ensues to conduct causal analyses and risk assessments and to design corrective actions. A verification process exists to track and enable the successful resolution of deficiencies, making sure that corrective actions are completed effectively and are properly documented. The sustainability of corrective actions is also verified during the subsequent yearly self-assessments.

Cyber Security

Sandia National Laboratories has three cyber environments:

- The Sandia Classified Environment (often referred to as "red") processes secret data of various categories and levels. It uses a separate infrastructure than that of our unclassified networks. Thus, Sandia's classified information systems are insulated from Internet attacks. The classified environment employs NSA-approved Type-1 encryption on dedicated lines for communication with approved DOE nodes.
- The Internal Restricted Environment ("yellow") stores all categories of unclassified information, including unclassified controlled information—for example, human resources information, project management data, export controlled information, and proprietary data. Controlled information is protected on a need-to-know basis by access control lists and other technical controls.
- The External Collaborative Environment ("green") is authorized to store non-sensitive unclassified information but is not authorized to store sensitive information unless additional technical controls are in place, such as encryption.

The yellow and green network environments both connect to the Internet and employ the same protective measures against Internet attacks.

All three environments are centrally managed and controlled. Thus we are able to technically enforce standards on all computers. Sandia's Network Information System stores data on every machine connected to our networks and is an enforcement tool for ensuring compliance across the laboratory.

Sandia's information networks and systems are certified and accredited in accordance with NNSA's Program Cyber Security Plan, which provides specific security requirements for information systems. All Sandia networks and systems are certified by Sandia's Cyber Security Site Manager and accredited by the NNSA Designated Authorizing Authority.

The "DOE Office of Independent Oversight Cyber Security Inspection" in August 2007 resulted in ten findings, and corrective actions were structured among 26 milestones. We are on track to complete all milestones.

Our unclassified computing environments (green and yellow) are attacked relentlessly. On a typical day, they are bombarded with a quarter million questionable events; after filtering and analysis, tens of thousands of those are established as malicious. Fictional networks that we set

up as targets attract thousands of probes, and we see increasing ingenuity in their design. We typically block 80 percent of the e-mail messages that come to us via the Internet; 92 percent of it is spam, the remainder is malicious email, and much is infected with viruses. Several cyber attempts each day meet the criteria for reportable events to DOE.

Sandia has taken many steps to improve cyber security in response to increased threats. Two-factor authentication is now required for e-mail or access to Sandia's Internal Restricted Environment (yellow) from remote locations. We have augmented commercial e-mail filtering to block malicious software (malware) and deployed technology to identify malicious internet sites that are counterfeit or deceptive. Sandia is aggressively implementing NNSA's diskless classified computing initiative, which includes blocking USB ports and substituting diskless workstation in place of personal computers on classified networks. This initiative will be complete by the end of September.

Sandia's computer security systems isolate cyber attacks and permit our experts to analyze intrusions quickly. Computers identified as possibly engaging in suspicious activity are forensically analyzed and, when necessary, taken off-line for advanced analysis. Appropriate actions are taken to ensure that other systems are not impacted by similar attacks or vulnerabilities. Affected users are notified, and computer system managers are continuously informed of current threats. The results of our forensic analysis are shared with other NNSA laboratories, defense community entities, and law enforcement.

Sandia has completed steps for accreditation of its node of the NNSA Enterprise Secure Network (ESN). ESN will provide a secure capability for classified electronic access among NNSA sites. Sandia had substantial input into the development of the ESN architecture and was the primary contributor to the ESN security plan.

Our strategy for cyber security is designed to engage users in doing a better job of protecting unclassified information, since attacks via the Internet do have the potential to access controlled information. Our internal security management teams continuously assess the evolving risks and threats to our networks and proactively upgrade our defenses with new tools and processes.

We are elevating our focus on the insider threat. Need-to-know controls are in place to protect unclassified controlled information. Upon logging-in to any Sandia network, the user is informed and must acknowledge that he has no expectation of privacy on his usage and that

everything he does on a government-owned computer system is subject to monitoring. And we do in fact monitor. We capture all transactions with the Internet from and to Sandia computers and subject that data to automated analysis for suspicious behavior. E-mails sent from a Sandia account to a foreign address are of special counterintelligence interest. To detect malicious insider activity, we often install software "trip wires" that alert us to unusual behavior. All privileged access (system administrators, database administrators, etc.) are required to use two-factor authentication.

I believe Sandia National Laboratories' cyber security program is among the most effective in the federal government. However, notwithstanding all the measures we take to protect our unclassified computing environments (both green and yellow), I acknowledge that penetration may occur despite our best efforts. Therefore, we evaluate that risk against the benefit of providing an unclassified computing environment that permits us to conduct laboratory operations in a modern, cost-effective way. We protect controlled content at a high level, and we assure that no content exists in our unclassified environment that could compromise our nation's nuclear deterrent or security if captured. Consequently, it is my opinion that the security measures on our unclassified computing environments provide an appropriate balance between protection and productivity.

Security Improvement Initiatives

Management at Sandia has strived to go beyond compliance as the main objective and to achieve a security program that is driven by performance goals. We have several initiatives in progress that bring focus to targeted issues where improvement is needed. In March 2007 we kicked off our initiative to review the security footprint at Sandia sites, followed in April by our campaign to reduce classified holdings—both consistent with mission needs. In September 2007 we ordered the lab-wide conversion to diskless workstations on classified networks; in the same month we initiated the rejustification program for vault-type rooms. We also have ongoing programs to improve corporate root-cause analysis, classification awareness, and control of prohibited articles.

On May 15, 2008, I received a letter from the director of the Office of Enforcement at the DOE Office of Health, Safety, and Security. Although the letter was not a formal

enforcement action, it raised concerns about the number of security incidents across DOE sites. The Office of Enforcement's concerns are valid, and we are taking deliberate action to address these concerns.

Based on the concerns expressed in the enforcement letter, we have initiated a lab-wide Security Performance Improvement Project (SPIP) to identify the underlying causes for the continuing security incidents and identify actions that will prevent or mitigate future incidents. Six teams were established to develop specific improvement actions in the following areas: management systems, classified e-mail on unclassified systems, protection of classified files on servers, protection of classified matter, introduction of controlled articles (especially cell phones) to secure areas, and accountability. All teams have completed initial assessments and evaluated root causes. Due to the nature of many of the security incidents, human factors experts are engaged with each team.

I have involved Sandia's senior management in this effort. The laboratory leadership team completed a case study exercise to identify actions within each corporate division that will further reduce incidents, including setting corporate reduction targets for security incidents by division. I require division vice presidents to identify actions and best practices that will help achieve the objectives of this project. Divisions will document their actions and progress in their quarterly Management Assurance Reports.

The power of modern communication technology and computer hardware have challenged security programs across the federal government as never before. We used to think of security as something that could be managed well with robust physical controls. In past decades that was largely true. But today the balance has shifted and the risk is greater on the cyber side than the physical side.

Unfortunately, the balance of resources between physical and cyber security has not been adequately adjusted to reflect that shift, in my opinion. We have done much to reduce the costs of physical security—by removing special nuclear materials, reducing classified holdings, and managing our security footprint, for example—and I believe we can live with a leaner posture for physical security. But to provide security against increasingly sophisticated attacks, cyber defense needs more resources. I was not surprised to learn that Deputy Secretary of Defense Gordon England sent a request to Congress in July asking to shift resources to computer security.

This is an issue that federal agencies are beginning to realize requires more emphasis.

Addressing the Cyber Security Challenge

The cyber threat is a national problem affecting information systems in government as well as the private sector. Given the importance of cyber security to the NNSA complex and the nation, Sandia is actively engaged in understanding the threat and developing technology, systems, and expertise to counter these threats, not only for Sandia, but also for DOE and other national security institutions.

Sandia's growing role in national cyber defense is consistent with its historic mission responsibilities in security systems research and development for DOE and other agencies. We are the design agent for all elements of DOE's transportation safeguards system, a responsibility for Sandia since the 1970s. Similarly, we have partnered with elements of the Department of Defense for decades to develop advanced security technologies for nuclear weapons throughout their life cycle. Our security expertise also contributes to international programs to improve nuclear materials protection and discourage proliferation. In recent years Sandia's programmatic security work has increasingly involved cyber defense, largely because federal missions and civil infrastructures now depend heavily on computer-based systems. Consequently, our research organizations have developed an institutional capability to detect cyber vulnerabilities and to mitigate them.

In September 2007, Sandia worked with DOE to organize the first DOE Summit Conference on Cyber Security. The event stimulated dialog among key stakeholders in DOE on the cyber threat and began the process of developing a broader strategy for cyber-related security issues. It became clear that the NNSA laboratories possess expertise that is highly relevant to this national problem. Subsequently, Sandia supported DOE in a second Cyber Security Summit which allowed the insights and learning derived from efforts started in the first Summit to be shared across a larger set of DOE's organizations.

Sandia's experience in cyber security is a resource for DOE and its laboratories and across many sites. We have worked hard to develop strong teaming relationships across the DOE Complex. Our forensic analysis, incident remediation, and response capabilities are sought out from throughout the complex, as evidenced by requests to assist other sites. Sandia led a tri-lab

simulation exercise in February to model a major cyber security incident involving multiple sites. The simulation demonstrated the incident-response approach that each site applies against cyber attacks and revealed clear benefits of collaboration. Sharing information, resources, and expertise will positively impact the incident-response efforts for participating sites.

Long-term success against the cyber threat will require a steady flow of highly skilled cyber security experts. We recognized some time ago that there were not enough of these people in the pipeline to give us assurance that those skills will be available as today's experts retire. Since 1998 we have offered a "Cyber Defenders" internship program in collaboration with local universities. The mentors and staff of the Cyber Defenders program provide students with cutting-edge research projects while instilling them with new skills. Sandia's Center for Cyber Defenders currently employs nearly 20 students who represent some of the most knowledgeable and passionate students in their field.

The national cyber threat is complex and touches multiple government agencies. It should be addressed through an integrated, government-wide response. I believe Sandia and the DOE laboratories can contribute significantly to the government-wide effort.

Concluding Remarks

Sandia has a longstanding culture of respect for security that is fundamental to our mission. We strive to comply with all applicable directives and requirements, with compliance as the essential baseline from which we advance our security performance. The security program at Sandia is structured with clearly stated lines of authority, responsibility, and accountability. We have done much to reduce the costs of physical security—by removing special nuclear materials, reducing classified holdings, managing our security footprint, and other initiatives. Sandia and its sister laboratories in DOE face a full spectrum of threats from multiple sources and encompassing multiple avenues of attack. The cyber security threat to the nation is especially difficult to manage, and it will require a concerted national response.

Mr. STUPAK. That concludes the opening statements. We'll go to questions. We're going to go 10 minutes.

I think we'll have votes coming up; maybe we can get our questions in before that.

Dr. Anastasio, if I may, GAO testified on the first panel that Los Alamos pulled the access to foreign nationals to the yellow network. Is that correct?

Mr. ANASTASIO. No, that's not correct.

Mr. STUPAK. It's not?

Mr. ANASTASIO. Foreign nationals do have access to our yellow network.

But we have a number of protections in place to ensure that proper care is taken. We do counterintelligence assessment of every individual. We have security plans and a very significant process we go through.

Mr. STUPAK. Do you have encryption on some of the more sensitive parts that are on your yellow?

Mr. ANASTASIO. We have some encryption on the more sensitive parts that are on the yellow network, and we have segmentation that we've put in place and we're further proceeding with that.

Mr. STUPAK. All right.

Dr. Miller, do foreign nationals have access to the yellow information? The yellow network, I'm sorry.

Dr. MILLER. Yes, sir. Just like Dr. Anastasio, we currently do have foreign nationals on our network. As I indicated in my testimony, we are in the process of creating another network. It was just—we did a pilot last year. It was just credited by NNSA about a week ago. So this fiscal year we will be creating a separate network for all of our foreign nationals that is separate from the yellow network.

Mr. STUPAK. All right. Would some of the information on your yellow network go on this new network you're—

Dr. MILLER. Yes, sir. I mean, for instance, all of the training requirements that are completely unclassified are required by—the foreign nationals require access to the training requirements. So the training courses, things like that that they require access to, will be on the blue network. So there will be some information that is transmitted.

Mr. STUPAK. Dr. Hunter, how about yourself, the foreign nationals on your yellow network?

Dr. HUNTER. On our yellow network we have about 11 foreign nationals that have some access in the appropriate areas, but none are from sensitive countries and I think the DOE requirement for the future is about sensitive countries.

Mr. STUPAK. Let me ask this question, if I may—Dr. Wilbanks, if I may.

The Director of Los Alamos noted in his opening statement that cyber threat is the greatest security concern. Would you agree that this is perhaps the greatest security concern facing DOE labs at this point in time?

Ms. WILBANKS. I can only speak from the cyber perspective. But, yes, sir, I would agree that it's a very high threat.

Mr. STUPAK. Well, let me ask you—to point that to the point that you can in open session here—what's the level of sophistication of these attacks? Are they increasing in capability?

Ms. WILBANKS. Yes, sir. I would be happy to elaborate in a closed session, sir.

Mr. STUPAK. Mr. Borgia, Ms. DeGette asked the question earlier—let me ask you this if I can.

Has a full inventory of the information residing on the unclassified networks of DOE national labs been inventoried?

Mr. BORGIA. No, not that I know of.

Mr. STUPAK. The other panel didn't necessarily think it was necessarily a wise choice. Do you it would be?

Mr. BORGIA. I think that I would defer to that answer.

I think the most important thing to do with this information is to be able to stop the intrusion, if it's possible. But to be able to catalog that information would be—that would be a tremendous library of cataloging we would be responsible for doing in the Department, and it would be overwhelming.

Mr. STUPAK. Let me ask you this question, if I may.

You testified that your work is closely coordinated with DOE's Office of Chief Information Officer and NNSA's Office of Chief Information Officer, and that you maintain strong, mutually supportive relationships in the cyber security. Yet for the past 3 years the Office of Inspector General has reported that the Department has failed to adequately address cyber security coordination and communication.

From a counterintelligence point of view, are you satisfied with the coordination and communication between the Counterintelligence and Information Technology Divisions in the DOE complex regarding the reporting of cyber incidents? And what, if anything, can be done to improve coordination and communication?

Mr. BORGIA. Yes. Thank you, Mr. Chairman.

I would have to say the answer to that is yes. There has been a substantial increase in the communication between my office and the chief information officers in cyber security. We—in the 2 years I've been here, we've had increasing contact with these offices—daily contact, weekly meetings, sometimes twice weekly meetings where we sit down and review matters of classified concern.

And there is continuing contact at the executive levels in each of these offices too. Dr. Wilbanks and Mr. Pyke and myself and their executive management staffs and mine are very, very familiar with one another, and we talk very frequently.

Mr. STUPAK. Let me ask this question, if you can answer it or if we have to go to a closed session, just let me know.

Mr. Podonsky and his group said they're not very sophisticated in cyber security, but yet they're able to get in with his Red Team and take control of—I don't want to say take "control," but have pretty good access in two science labs. And everyone is telling me today it is more sophisticated. It's a great concern.

Is it possible that there have been breaches of our cyber security that we don't know about? Is the sophistication—the level of sophistication—in other words, like when I play basketball, are you above the rim or not?

I'm below the rim, believe me. But are there teams above that rim that we possibly don't even know about?

Mr. BORGIA. Yes.

Mr. STUPAK. OK. I have more questions, but I'm going to ask those in closed session on that aspect of it.

Let me ask this. We've talked a little bit about this yellow network. And let me—in light of that answer, Mr. Borgia, what is NNSA's opinion on the network access that's been provided to foreign nationals? What control does, like, let's say, Los Alamos have in place to ensure that foreign nationals have a need-to-know for the access they have been provided with on the network?

Mr. BORGIA. Sir, perhaps the lab director or NNSA would be better to answer that question.

Mr. STUPAK. OK.

Dr. Wilbanks, do you want to add anything to that question?

Ms. WILBANKS. The labs have done a great job in segregating various components within their yellow network that allows their foreign nationals on there.

Excuse me. As you heard, Lawrence Livermore is building a separate network for the foreign nationals. They take great strides to limit the access of the foreign nationals to specific areas of information, and then to limit their access within the network itself.

Mr. STUPAK. My concern—I guess I brought it up earlier in the first panel—was that mosaic approach. You take something that doesn't seem real sensitive. It's on the yellow. So I take a piece here, take a piece there, put it together, does it become then sensitive, that we should have greater restrictions?

Do you care to comment on that, Dr. Anastasio?

Mr. ANASTASIO. Let me indicate that before we have any foreign national on our network, we go through a very extensive review, including a counterintelligence review of those individuals before we allow them on. We're essentially moving to do the same thing Lawrence Livermore is doing in their blue network to have a separate network that's segregated in a way that allows the foreign national to have access only to the information they need, as I said in my testimony.

And the other thing is that the yellow network has many protections on it. It's segregated in a sense already to be the network we use for information that's beyond what would be revealed to the general public. Before we put any information on that network, we go through an extensive classification review before that information is allowed to be on the network.

But then, beyond that, the mosaic issue is always a challenge. And it's something they watch out for as we go and do our reviews of the information and as we look at any issues that may arise.

But, yeah, I think we are very vigilant about these issues.

Dr. MILLER. Mr. Chairman, if I could just add a slight amplification of that in the sense of an example.

Personally identifiable information is obviously something we're all very sensitive to. That information is separately segregated and protected on the yellow network. So, for instance, I do not have access to the PII of all of the employees at the laboratory; it is separately segregated. The number of people who have access to it is

limited to a very small number who actually are required to be able to do that in concert with their job.

An example of why somebody might want to have access to it is, if an employee were taken to the medical facility in an emergency, the medical people need to be able to get access to personal information about what drugs, whatever. So there are specific circumstances under which people could get access, but generally the information is very tightly segregated, based upon the function and based upon the need to know of the rest of the people.

Mr. STUPAK. But you don't—on your yellow networks you don't have anything where you catalog what foreign nationals are looking at or working on, do you?

Mr. ANASTASIO. We're very—we keep—as Dr. Hunter said, we keep a full record of all the in-going and out-coming traffic on our network and we watch that and search it. And we have sensors deployed to look at the traffic that's going on. And we periodically do scans, as well as do scrubs of the information that's moving around, to ensure ourselves that the proper behavior is going on on the network.

Mr. STUPAK. OK.

Dr. Wilbanks, let me ask you one more question, if I may. If information was being exfiltrated from any of the DOE labs, would this be detectable? In other words, does DOE have the ability to fully understand whether information is being lost from any of the DOE labs' networks?

How would they know this?

Ms. WILBANKS. DOE, NNSA and the site offices themselves have many sensors that monitor the outgoing traffic. And there are techniques, technologies to determine what information is being exfiltrated. I'd be happy to elaborate, sir, in a closed session.

Mr. STUPAK. But it's possible the sensors don't pick up what's being exfiltrated, right? It just depends on—

Ms. WILBANKS. Yes, sir. That's always a possibility we face.

Mr. ANASTASIO. Excuse me, Mr. Chairman. Just to amplify on that, we do have layers of defense, though. I think that's important.

Although no layer is perfect, we have sensors that we use inside the laboratories. We have—NNSA has a set of techniques that they use, DOE and then even the broader national security community. So we rely on all those layers to allow us to know what's going on, and if we have a problem, how we can react.

Mr. STUPAK. Sure. I agree with that. But the attacks are becoming more and more sophisticated. And if we're playing above the rim, you're not going to know.

Mr. ANASTASIO. But our job as a national laboratory is to have the innovation and creativity to stay ahead of the game, to be leading the world on these activities and to draw on the full resources of all the elements of the government to do our job.

So we're very conscious, and Dr. Hunter, I thought, was very eloquent about the people, that that is a key issue for us to make sure we have those people that can be at the state of the art, ahead of the state of the art.

Mr. STUPAK. I don't disagree with any of that. But then when we see reports from other offices indicating that our cyber security is

sort of lacking, and if this is our 14th hearing over the last 8 years, when it comes to security, I'm very concerned—not just the physical, but maybe more so the cyber security which has taken on greater significance.

And if our enemy is getting more sophisticated—well, I hope we're above the backboard, not above the rim. I'm not real confident we are at this point in time.

Dr. Hunter, and then I'm going to go to Mr. Shimkus.

Ms. WILBANKS. Mr. Chairman, if I may elaborate, please, sir.

One of the things I mentioned in my opening statement was the fact that DOE and NNSA have now combined in their incident management, incident handling and identification to help keep us above the backboard, sir.

Mr. STUPAK. Right.

Dr. Hunter.

Dr. HUNTER. Thank you, Mr. Chairman.

Mr. STUPAK. Turn that mic on, please. I'm sorry.

Dr. HUNTER. Mr. Chairman, we've all acknowledged the rightful concern about the cyber issue, as you just stated.

One point I would like to add to what he just said: The laboratories and the DOE are working very closely together so they pool their expertise. If there's any evidence, as we watch very carefully, of things that might have been or could be exfiltrated, these people call each other and quickly analyze and try to understand the situation. In a way—so it's like a big team. When you address one place, you get the team of the other place that's quickly providing the benefit of their experience to try to understand what is happening and to respond to it.

Mr. STUPAK. I agree you're doing all that. I hope it works, but when I get figures like 400 million attacks a month, that's almost impossible to keep on top of. So I hope those sensors and filters really are doing their job.

Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman.

I think you can continue to hear from Members of Congress, hope that security is improving; but you also hear great skepticism over the years of Members being involved in some pretty big breaches.

Let me ask the three directors of the labs, because, Dr. Miller, you mentioned a blue network. Or the—all labs being unique, as I understand, Dr. Anastasio, Dr. Hunter, are you developing blue networks? Are there best practices? Do you communicate and share information to make you all better?

Mr. ANASTASIO. Yes, sir, very much.

And so at Los Alamos we—as I said, we're building a further segmented element of our segmented network on our yellow network. That's conceptually equivalent to what Lawrence Livermore is doing with their blue network. We haven't given it a name of a color; it's essentially the same thing. But—we're using slightly different approaches to accommodate the differences we have, but it's really the same thing.

But as far as sharing goes, absolutely we share—we, the three of us, talk together. We've talked about this issue for years amongst ourselves, about how to approach it. Even more important, our technical staff is in constant contact with each other.

When we had a concern about a penetration of the yellow network, we had, in fact, people from Sandia to come up to Los Alamos to actually work in our team. So it's an example of how we're working together.

Mr. SHIMKUS. The other thing is time frame. When we're talking about sensitive information and—yeah, good lessons learned; you're sharing information—time.

Dr. Anastasio, I'm going to come back to you. But let me finish with Dr. Miller and Dr. Hunter. And then I'm going to come back to Los Alamos.

Dr. MILLER. Yes. I think the question you raise is a very important one. And as Dr. Anastasio said, we work very, very hard. We're very cognizant of the technical approaches that both Los Alamos and Sandia have taken. They have developments that—we are watching very carefully; when those developments mature to the point where they can be adequately assessed, we will frequently move those across from one laboratory to the other.

We share people. We share information. So there's a very, very tight coupling between the three of us and again, as we have said before, with the NNSA/DOE and the much broader Federal community in this area.

Dr. HUNTER. Thank you. I think I commented on the sharing and the working together. I will comment on your specific question about the best practices.

The existence of a three-level network—the unclassified, the yellow network, as we just described and the classified—is, in fact, a best practice developed by the laboratories, which we feel is somewhat unique and important.

Secondly, we have not decided to go to a blue network at this point. But what we have decided to do is much like what Mike Anastasio said, emphasize stronger segmentation of the yellow network to really be sure the need-to-know controls are in place, and emphasize then monitoring of information coming and going into that network.

And then finally to really look at this question of what do foreign nationals particularly need in terms of their requirements to work at the laboratory, say, on broad science? Sometimes it's limited to things like payroll and benefit information, which you can really segment very strongly.

So the combination of those things, we think, will lead us to the proper decision.

Mr. SHIMKUS. And let me follow up.

We don't want to get too—you know, just put all the burden on the foreign national debate, because a lot of our security breaches would—you know, are nationals—you know, born U.S. citizens. But, you know—and we—you know, this list is public on some of these. But the vetting process for those, I mean, they're still citizens of countries that we have identified as sensitive or nonsensitive. So the vetting has to be as good as we do when we give our security clearances, I would assume.

Let me go to Mr. Borgia to respond to the vetting process of the individuals who are hired, both alien, visitors and citizens.

Mr. BORGIA. Sir, there is a vetting process that counterintelligence uses to look at foreign nationals who are coming into the complex.

However, I think it would be better to talk about that in a classified setting, to give you a more detailed understanding of what we do. The security program is responsible for conducting backgrounds of other persons who are hired, you know—

Mr. SHIMKUS. And that's fine. We'll have that opportunity. So thank you.

Let me go to Dr. Anastasio because you're the one who obviously was the subject of the most recent report. And I think our position is, anyone who's been, you know, in an executive position and you—and the inspector general comes down or—in the military, a former Army officer or someone from the corporate headquarters, who is doing that same thing, they've identified numerous deficiencies.

I guess this thing was finally left in December. So then the compilation of the report, their analysis, finished just a month ago; and then this is a very recent—you know, a publication of September 2008.

So if we would go through it, you know, starting on page—although a risk assessment was completed, it was not comprehensive. Are we now able to say that the risk assessment is now comprehensive?

Mr. ANASTASIO. Yes, we are. As part of our process to get accreditation and verification with the process we have with NNSA, we have gone through a very formal set of risk assessments, and we are—for all our networks and all our activities on the yellow network, as well, of course, as the classified network. And we are just now completing that. We'll be done in December, and we'll finish the full accreditation and certification of all our systems.

But we've gone and taken other steps in response to the GAO.

Mr. SHIMKUS. I'll just keep following, because that's what you hear by Members, you know, guidelines. You know, if I was the—you know, the Secretary of Energy, I would say not good. These are the deficiencies. When will they be resolved? And I think that's where Members are.

So the other one is policies and procedures have shortcomings. Have the shortcomings been addressed?

Mr. ANASTASIO. Yes, sir, they have. Again, we've done a comprehensive look for all the issues that are—at least in the draft report. Since the final just came out today, I haven't seen the final, but we have certainly seen the draft report, and we are already responding to all of the issues that have been raised in that report, including more stringent protections, reducing the number of ports that are active, more robust cyber detection. We've changed our policies and made them more clear, as I said in my—and comprehensive—in my opening statement. And we're just addressing all those things.

Mr. SHIMKUS. OK. Because my time's short and there are going to be votes, so you understand the point. I would then just turn to the other directors. And it would make common sense for you all to review the report from that position and relook at your own processes and procedures.

Quickly, if you'd like to, sir.

Dr. MILLER. Yes. Again, we certainly are aware, have read the draft report and have reflected it on ourselves. We will do the same thing with the final report that just came out.

Mr. SHIMKUS. The primary job, other than passing the laws of the land—and we are justly criticized for not doing a good job in oversight. This is our job; this is what we're supposed to be doing. And so that's why we're continuing to be on this.

Sir, do you want to add?

Dr. HUNTER. Yes, sir.

I just agree. We share the same challenges, and we'll derive the same lessons learned from every activity.

Mr. SHIMKUS. You all were out with the rest of the folks when the first panel was being asked, and we did spend a lot of time on the yellow network. I did talk about e-mails and attachments and the Trojan horses and all these things that some of us are just getting to understand and those types.

A lot of the responses were that we monitor what is—my impression, just trying to pay attention, was, we monitor what's being sent out. We grab it, and we segregate it. We hold onto it.

So it just led me to the question, if we grab and hold onto it, do we grab and hold onto it before it gets out to the system, or it's going out the door, so we at least know what we lost?

Who wants to respond to that question? We know what we lost. Is that really what we're talking about?

Mr. PYKE. Mr. Shimkus, in quite a number of cases we are able to actually block the outgoing transmission before it takes place. There are occasions where we learn about it after the fact or block it when it's partway out. But we are able, through the collaboration that's been discussed by various members of the panel; and through an active collaboration with the counterintelligence folks, we are able to work together not just week by week, but in near real time, to use the information we have to block outgoing attempted exfiltration of information.

Mr. SHIMKUS. And Mr. Chairman, if I may, I just want to end up with—the inspector general testified about incomplete certification and accreditation. We're kind of raising some of that at the labs about incomplete implementation by the Department of Federal cyber security policies, especially for DOE and for NNSA.

What's your response to these findings?

Ms. WILBANKS. NNSA has implemented new policy as of May 2008 that completely strengthens the certification and accreditation process. It also strengthens some of the requirements and restrictions on the yellow network. And the labs are in the process of implementing this policy at this time.

Mr. SHIMKUS. Go ahead.

Mr. PYKE. Mr. Shimkus, if I may, we have a comprehensive set of requirements DOE-wide in the cyber security area; always, of course, looking to improve them and to add to them, but they are in place.

And it's my understanding in working with Dr. Wilbanks and her staff and my personal observations that NNSA not only follows these requirements, but given the nature of the mission of NNSA,

they frequently strengthen them to provide protection against the special risks faced by NNSA programs.

Mr. SHIMKUS. You know, the inspector general recommends time frames and benchmarks. I mean, would you agree with his recommendation? And if you do, do you have them? And if you do, would you supply those to the committee?

Ms. WILBANKS. Yes, sir. We do agree. Yes, sir. We do have them. And yes, sir, we will supply them.

Mr. SHIMKUS. Thanks. Thanks, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Shimkus.

Mr. Borgia, if I may, we had some questions of the first panel—Mr. Friedman, in particular—about the letter that was sent to Mr. Dingell by a former senior counterintelligence officer at Lawrence Livermore.

Are you familiar with that letter at all?

Mr. BORGIA. Yes, Mr. Chairman, I am.

Mr. STUPAK. What's your reaction to it, especially when they say that as a result of the changes, vulnerability of DOE personnel and facilities to hostile intelligence entities has increased exponentially?

Mr. BORGIA. I couldn't hear the first part of the—

Mr. STUPAK. That as a result of the changes at DOE, the vulnerability of DOE personnel and facilities to hostile intelligence entities has increased exponentially.

Mr. BORGIA. That would be wrong, Mr. Chairman.

Mr. STUPAK. That would be wrong?

Mr. BORGIA. Yes.

Mr. STUPAK. And the letter cites about five different examples.

Mr. BORGIA. Sir, I can give you in a classified hearing great examples of the success that this program is experiencing right now that collectively have not been experienced throughout the rest of the 10 years of the program.

We have an extraordinary marriage with the FBI. The FBI is dedicated, as I mentioned myself, but also 20 other special agents who are agents in the labs included—including agents in the weapons labs.

There has been—there's been extraordinary connection with the Intelligence Community. And this program today has a much bigger profile in the Intelligence Community. The national counterintelligence executive has identified this as one of the top four programs. He'd always talked about this in briefings on the Hill as the "top three programs."

Now he says the top four programs. That's DOE's counterintelligence program. There is a great new confidence in the counterintelligence program that is identified and experienced not only outside in the intelligence community, but I believe my colleagues in the Department as well as the Secretary and the NNSA Administrator would agree.

Mr. STUPAK. So you wouldn't agree that, if I can summarize what this individual who had 29 years experience with the FBI in this area, that the counterintelligence aspect of our security has been diminished while the intelligence gathering has increased at the expense of counterintelligence and DOE?

Mr. WILSHUSEN. Yes. That would be wrong.

Mr. STUPAK. That would be wrong?

Mr. WILSHUSEN. Yes. And, sir, I have almost 25 years in the FBI, worked counterintelligence, counterterrorism, and criminal investigative programs. I could sit, and I would be very happy to sit and talk about and give you the details in a classified setting about what the accomplishments of this program are.

Mr. STUPAK. Well, I wanted to raise it, and I am glad you are familiar with it because it probably will come up in our closed session, which we are going to go into soon.

Mr. Shimkus, questions, please.

Mr. SHIMKUS. Just a unanimous consent request for these two documents. I think the staff shared them with you. The one's a Foreign National Assignments with computer access. It just has a listing of all that. And another one, just to highlight the fact that we have U.S. citizens that are not good citizens also. There is a story today, an AP story: Scientist Accused of Selling Rocket Data to China, an AP story about that. I am asking unanimous consent to accept those.

Mr. STUPAK. Without objection, then—I'm looking for the date on this one here. Today's date, Scientist Accused of Selling Rocket Data to China, that will be made part of the record, that AP news story. And Foreign National Assignees With Computer Access, dated September 12, 2008, will also be made part of the record.

[The information appears at the conclusion of the hearing.]

Mr. STUPAK. That is going to conclude the open part of our hearing. We are going to have a couple votes on the floor, so why don't we do this: Instead of reconvening in 10 minutes, I think, let's shoot for 2:00. We have got at least three votes on the floor; they are going to call them here in a second, and then we can meet in 2218. So let's meet in Room 2218 of the Rayburn Building at 2:00. And only those individuals who have appropriate Top Secret/Q level clearances that have been previously sent to the committee clerk and the House security will be admitted. So I will dismiss this panel then.

And before we close this portion of the hearing, I ask unanimous consent that the hearing record will remain open for 30 days for additional questions for the record. Without objection, the record will be open.

I ask unanimous consent that Tabs 1 through 7 and Tabs 25 and 26, those nonofficial use only exhibits of our document binder, be entered into the record. Without objection, the documents will be entered into the record.

Mr. STUPAK. That concludes the open portion of this hearing. We will recess until 2:00 and reconvene in Room 2218 of the Rayburn Building for our closed portion of this hearing.

[Whereupon, at 1:13 p.m., the subcommittee recessed to proceed in closed session at 2:00 p.m. the same day.]

SEP 11 2008

September 1, 2008

[redacted]

Terry D. Turchie
[redacted]

Chairman John D. Dingell
House Committee on Energy and Commerce
2328 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Dingell:

I served as an FBI Special Agent for 29 years, retiring from the Bureau at the end of May 2001 as the Deputy Assistant Director of the FBI's Counter-terrorism Division. During my career with the FBI, I worked a variety of criminal and national security matters, which included counterintelligence and counterterrorism. I led the multi-agency Unabom Task Force, authored the search warrant affidavit for the mountain cabin of convicted Unabomber Theodore Kaczynski, and was assigned as the FBI Inspector-in-Charge of the fugitive hunt for convicted Olympic bomber Eric Robert Rudolph in the mountains of North Carolina from March 1998 until March 1999. Both Kaczynski and Rudolph pleaded guilty before trial for the crimes they committed, largely as a result of solid and unimpeachable evidence collected while the task forces were searching for them.

From June 2001 until September 30, 2007, I served as the Senior Counterintelligence Officer at Lawrence Livermore Nuclear Weapons Laboratory. Upon my retirement from LLNL, Thomas P. D'Agostino, Undersecretary for Nuclear Security and NNSA Administrator, had this to say in a letter (copy attached) dated September 28, 2007:

> *"You assumed responsibility for the LLNL CI Office in June 2001 and built it into the premier counterintelligence program within the National Nuclear Security Administration (NNSA) and, many would agree, within the Department. Your outstanding work was twice validated by an external inspection team, most recently in July 2007. These two inspections, covering your entire tenure as the SCIO at LLNL, resulted in overall 'Excellent' ratings."*

Prior to my departure, I made it clear to top level Lab managment; DOE's counterintelligence inspection team; representatives of the DOE Inspector General's Office; and leadership in the DOE Office of Intelligence and Counterintelligence that my decision to leave was based upon the dangerously chaotic state of counterintelligence within DOE. I emphasized the potentially catastrophic consequences of the new

direction the program was moving towards by restructuring around intelligence collection and away from sound counterintelligence principles.

In late September 2007, I sent two rather blistering emails to the DOE Office of Intelligence and Counterintelligence expressing my concern that the changes in progress and the restructuring was creating larger counterintelligence vulnerabilities within the Department. While I do not have copies of the emails, I have read with interest the recent report on counterintelligence within DOE and wish to notify you of my continuing concern that Congress is being misled on the true nature of the effectiveness of counterintelligence within the Department of Energy.

I strongly agree with a number of the concerns cited in the report. Since the consolidation of DOE and NNSA counterintelligence under the overarching Office of Intelligence and Counterintelligence within DOE, counterintelligence (CI) capabilities have been greatly undermined. As a result, the vulnerability of DOE personnel and facilities to hostile intelligence entities has increased exponentially.

Examples of these vulnerabilities are:

1.) After DOE and NNSA CI were reconsolidated, necessary, ongoing communication between Senior Counterintelligence Officers in the field and the Deputy Director of Counterintelligence was drastically reduced. The chief of NNSA Counterintelligence had held quarterly meetings with all of her field representatives, communicated with them by email at a minimum of a dozen times each month, and frequently talked with each of them by telephone regarding serious CI incidents and cases. The Deputy Director who replaced her held no meetings, sent no emails, and called me just several times in the two years before I left.
2.) The chief of NNSA CI consistently reached out to the NNSA laboratory directors, engaging them in the development of sound counterintelligence principles and encouraging their support and involvement in the CI programs at the labs. She understood that all of the labs were different, but recognized the importance of consistency, transparency, and team building with all levels of lab management. As a result, there was a substantial trust between the NNSA lab directors and the chief of NNSA CI which translated into programmatic initiatives, expeditious handling of CI vulnerabilities, and continuous employee awareness from the top down of the CI threat.
3.) The chief of NNSA CI, supported by a small, yet seasoned and pro-active CI team at the Headquarters level, worked tirelessly to acquire funding to secure the full staffing of CI positions throughout the field to uncover and deal with identified threats. Since the reconsolidation, field CI positions have been severely reduced. As I prepared to retire as the LLNL Senior Counterintelligence Officer (SCIO), I located and groomed a highly qualified candidate acceptable to the lab director for the position. One year later, in spite of the fact that LLNL has undergone significant and inevitably disruptive management change, no SCIO has been named. The 2007 DOE CI inspection of the LLNL CI program concluded that the

program needed additional positions and that vacated positions should be filled immediately. The DOE Deputy Director of CI has ignored those inspection recommendations repeatedly. In fact, I never received a response of any type from DOE Headquarters to the second consecutive finding of "excellent" for the 2007 CI inspection.

4.) After the consolidation, the Deputy Director for CI told me first hand that he had no control over the CI budget, did not have any idea how much money he had to spend or where it was located, and couldn't get any answers from DOE Director of Intelligence and Counterintelligence Rolf Mowatt-Larsen or his staff as to the CI budget. At a conference in Las Vegas in the spring of 2007 sponsored by Mowatt-Larsen, I raised the budget issue during a rare one hour session involving the senior counterintelligence officers and the Deputy CI Director. His response was to look down at his watch and remind all of us that there was a "social" in Mowatt-Larssen's hotel suite, so we better wrap it all up so we could be there on time.

5.) The DOE Director of Intelligence and Counterintelligence, Rolf Mowatt-Larsen, is a former CIA officer who is intent on the primacy of intelligence over counterintelligence. Since the creation of the new structure under Mowatt-Larsen:

   a.) The DOE Counterintelligence Budget, personnel staffing, training, analysis, cyber threats, and computer management related counterintelligence issues are under his management.

   b.) As a result, the focus of counterintelligence analysis in the field has become almost exclusively strategic and based upon intelligence collection and the production of intelligence information reports, de-emphasizing tactical analysis to support the identification of counterintelligence issues.

   c.) The budget for computer security matters at the labs has been reduced substantially, creating both security and counterintelligence vulnerabilities.

   d.) Considerable money has been spent to relocate Field counterintelligence programs into closed and classified SCIFs and to merge counterintelligence cyber information systems with the intelligence information system. This is consistent with an intelligence analysis approach, but totally inappropriate for the effective operation of a counterintelligence program that relies on continuous contact with the lab population where counterintelligence vulnerabilities reside. Ironically, it also increases the potential pool of individuals throughout the DOE Office of Intelligence and Counterintelligence who have access to sensitive counterintelligence information.

   e.) All of these changes have occurred without any written strategy documents and in an atmosphere completely lacking written polices, guidelines, and rules. In fact, the only matter ever discussed with the Senior Counterintelligence Officers by the Director of the Office of Intelligence and then vigorously pursued by his staff was the need to

change Executive Order 12333 to give more latitude for "intelligence operations" at the lab level.

f.) Counterintelligence awareness at the field level has been significantly diminished as an objective, whereas previously it was a critical foundation of the program. It has been replaced by an atmosphere of suspicion and distrust, which is permeating the overall counterintelligence program as a result of the creation of the Office of Intelligence and Counterintelligence.

Perhaps most disturbing is the purge of over two dozen people from key counterintelligence positions within the DOE complex over the past two years as these changes have occurred. Highly experienced individuals have been fired, resigned, retired early, or have been reassigned to other positions within the DOE or NNSA because they dared challenge some of Mowatt-Larsen's changes based on their concern for the rule of law or the dramatic and disastrous impact his changes have had on DOE counterintelligence overall. There is no room for dissenting opinions and they are in fact viewed as disloyalty.

At one meeting, a key advisor to Mowatt-Larsen summed it up this way, as closely as I can remember;

> *"The train has left the station. Some of you will disagree with the changes, some of you will leave, some of you will get sick and I suggest you leave as well for the good of your health. But the time for disagreement is over and you will do as directed."*

I strongly encourage the appropriate committees of the United States Congress to hold hearings on the current status of counterintelligence within the Department of Energy. Since the reconsolidation of the DOE and NNSA counterintelligence programs and the creation of the Office of Intelligence and Counterintelligence, the counterintelligence mission at the national labs and throughout the DOE has been turned into a massive intelligence collection program, with the creation of a host of attendant counterintelligence vulnerabilities. Based on my own extensive and successful professional experience in the fields of both counterintelligence and counterterrorism, I have little doubt that this has opened the way for major security breaches involving DOE installations and personnel in the future.

Sincerely,

Terry D. Turchie

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

September 28, 2007

OFFICE OF THE ADMINISTRATOR

Mr. Terry D. Turchie
Senior Counterintelligence Officer
Lawrence Livermore National Laboratory

Dear Mr. Turchie,

With the time until your retirement now measured in hours (instead of years, months or days) I want to take a moment to reflect on your significant contributions as Senior Counterintelligence Officer (SCIO) at the Lawrence Livermore National Laboratory (LLNL).

You assumed responsibility for the LLNL CI Office in June 2001 and built it into the premier counterintelligence program within the National Nuclear Security Administration (NNSA) and, many would agree, within the Department. Your outstanding work was twice validated by an external inspection team, most recently in July 2007. These two inspections, covering your entire tenure as the SCIO at LLNL, resulted in overall "Excellent" ratings.

Your successes were many. Five years ago your office first alerted this Department to a significant cyber issue and you then pioneered counterintelligence (CI) investigative approaches to deal with it. The result was substantial mitigation of the threat at LLNL and across the government. Your program led all other CI offices in the collection and dissemination of Intelligence Information Reports, with numerous kudos received from recipients throughout the United States Intelligence Community. You have helped LLNL and NNSA manage the risks posed by our significant international interactions, earning a great reputation for sound judgment and excellent advice.

On behalf of all the men and women of NNSA, I want to thank you for your steadfast dedication to CI and national security. We in NNSA were fortunate to have the benefit of your experience and expertise, developed over the course of your career with the Federal Bureau of Investigation. Your outstanding personal qualities and professional capabilities, much appreciated by us, are now evident to all who may read your new book, Hunting the American Terrorist. Best wishes for continued success.

Sincerely,

P. D'Agostino

Thomas P. D'Agostino
Administrator

Associated Press

Related News

FBI swoop on 'China space spy guy
Nature.com (subscription) - 31 minutes ago

US man charged with exporting space data to China
Reuters - 15 hours ago

Virginia Physicist Arrested for Illegally Exporting Space Launch ...
MarketWatch - 15 hours ago

Full coverage »

Scientist accused of selling rocket data to China

14 hours ago

NORFOLK, Va. (AP) — A scientist who heads a high-tech company in Newport News has been charged with illegally selling rocket technology to China and offering bribes to Chinese officials, federal prosecutors said Wednesday.

Shu Quan-Sheng, 68, made an initial appearance in U.S. District Court in Norfolk and is being held in jail until a bond hearing Monday.

Shu, the president of AMAC International Inc., is charged with two counts of violating the federal Arms Control Act and one count of bribery. If convicted, he faces up to 10 years on each arms count and five years for the bribery charge.

It could not be determined whether Shu has hired a lawyer. A phone message left at his company was not returned.

According to a criminal complaint unsealed Wednesday, Shu sold technology to China for development of hydrogen-propelled rockets. The Chinese government is developing a space launch facility in the southern island province of Hainan that will house liquid-propelled launch vehicles designed to send space stations and satellites into orbit.

The complaint also accuses Shu of bribing Chinese officials to award a $4 million hydrogen liquefier contract to a French company acting as an AMAC intermediary.

Shu is a naturalized U.S. citizen who was born in Shanghai. His company also has offices in Beijing.

Federal authorities in recent years have prosecuted more than a dozen cases of either traditional spying or economic espionage related to China. U.S. officials have warned in the last year of increasing espionage efforts by Beijing.

Hosted by Google

Total DOE Foreign National Assignees
12-Sep-08

Facility	Country	Assignees
Advanced Mixed Waste Treatment Project	Iraq	1
Advanced Mixed Waste Treatment Project	United Kingdom	2
Albany Research Center	China, People's Republic Of	1
Albany Research Center	India	1
Albany Research Center	United Kingdom	1
Ames Laboratory	Algeria	1
Ames Laboratory	Australia	3
Ames Laboratory	Austria	1
Ames Laboratory	Bangladesh	1
Ames Laboratory	Brazil	1
Ames Laboratory	Bulgaria	1
Ames Laboratory	Burkina Faso	1
Ames Laboratory	Canada	2
Ames Laboratory	China, People's Republic Of	131
Ames Laboratory	Czech Republic	3
Ames Laboratory	Ecuador	1
Ames Laboratory	Egypt	1
Ames Laboratory	France	4
Ames Laboratory	Germany(Unified)	11
Ames Laboratory	Greece	4
Ames Laboratory	Guatemala	1
Ames Laboratory	Hungary	1
Ames Laboratory	India	48
Ames Laboratory	Indonesia	1
Ames Laboratory	Ireland	1
Ames Laboratory	Israel	4
Ames Laboratory	Italy	1
Ames Laboratory	Japan	5
Ames Laboratory	Korea, South	31
Ames Laboratory	Lebanon	1
Ames Laboratory	Lithuania	1
Ames Laboratory	Mexico	2
Ames Laboratory	Nepal	2
Ames Laboratory	New Zealand	2
Ames Laboratory	Norway	2
Ames Laboratory	Poland	4
Ames Laboratory	Romania	3
Ames Laboratory	Russia	11
Ames Laboratory	Serbia, Republic of	2
Ames Laboratory	Slovakia	1
Ames Laboratory	Spain	1
Ames Laboratory	Sri Lanka	2
Ames Laboratory	Sweden	1
Ames Laboratory	Taiwan	13
Ames Laboratory	Thailand	2
Ames Laboratory	Trinidad and Tobago	1
Ames Laboratory	Turkey	8
Ames Laboratory	Ukraine	7
Ames Laboratory	United Kingdom	2
Ames Laboratory	Venezuela	2
Ames Laboratory	Yugoslavia, Federal Republic of	2
Argonne National Laboratory-East	Albania	2
Argonne National Laboratory-East	Algeria	4
Argonne National Laboratory-East	Argentina	26
Argonne National Laboratory-East	Armenia	4
Argonne National Laboratory-East	Australia	205
Argonne National Laboratory-East	Austria	22
Argonne National Laboratory-East	Azerbaijan	4
Argonne National Laboratory-East	Bangladesh	11
Argonne National Laboratory-East	Barbados	1
Argonne National Laboratory-East	Belarus	15
Argonne National Laboratory-East	Belgium	22
Argonne National Laboratory-East	Bolivia	2
Argonne National Laboratory-East	Bosnia-Herzegovina	4
Argonne National Laboratory-East	Brazil	33
Argonne National Laboratory-East	British Indian Ocean Territories	2
Argonne National Laboratory-East	Bulgaria	27
Argonne National Laboratory-East	Burma	3
Argonne National Laboratory-East	Cameroon	3
Argonne National Laboratory-East	Canada	302
Argonne National Laboratory-East	Chile	5
Argonne National Laboratory-East	China, People's Republic Of	815
Argonne National Laboratory-East	Colombia	18
Argonne National Laboratory-East	Costa Rica	1
Argonne National Laboratory-East	Cote D'Ivoire(Ivory Coast)	1
Argonne National Laboratory-East	Croatia	2
Argonne National Laboratory-East	Cyprus	2
Argonne National Laboratory-East	Czech Republic	14
Argonne National Laboratory-East	Denmark	47
Argonne National Laboratory-East	Dominican Republic	1
Argonne National Laboratory-East	Ecuador	4

Argonne National Laboratory-East	Egypt	7
Argonne National Laboratory-East	El Salvador	1
Argonne National Laboratory-East	Estonia	1
Argonne National Laboratory-East	Ethiopia	6
Argonne National Laboratory-East	Fiji	1
Argonne National Laboratory-East	Finland	10
Argonne National Laboratory-East	France	169
Argonne National Laboratory-East	Gambia	1
Argonne National Laboratory-East	Georgia	6
Argonne National Laboratory-East	Germany(Unified)	326
Argonne National Laboratory-East	Ghana	4
Argonne National Laboratory-East	Greece	19
Argonne National Laboratory-East	Guatemala	2
Argonne National Laboratory-East	Guyana	1
Argonne National Laboratory-East	Honduras	7
Argonne National Laboratory-East	Hong Kong	8
Argonne National Laboratory-East	Hungary	23
Argonne National Laboratory-East	India	468
Argonne National Laboratory-East	Indonesia	10
Argonne National Laboratory-East	Ireland	17
Argonne National Laboratory-East	Israel	55
Argonne National Laboratory-East	Italy	107
Argonne National Laboratory-East	Jamaica	5
Argonne National Laboratory-East	Japan	167
Argonne National Laboratory-East	Jordan	13
Argonne National Laboratory-East	Kazakhstan	5
Argonne National Laboratory-East	Kenya	7
Argonne National Laboratory-East	Korea, South	228
Argonne National Laboratory-East	Kuwait	1
Argonne National Laboratory-East	Kyrgyzstan (Kyrgyz Republic)	1
Argonne National Laboratory-East	Laos	1
Argonne National Laboratory-East	Latvia	4
Argonne National Laboratory-East	Lebanon	5
Argonne National Laboratory-East	Lithuania	6
Argonne National Laboratory-East	Luxembourg	1
Argonne National Laboratory-East	Macedonia, The Former Yugoslav Republic of	3
Argonne National Laboratory-East	Malaysia	8
Argonne National Laboratory-East	Mexico	62
Argonne National Laboratory-East	Mongolia	1
Argonne National Laboratory-East	Montenegro	1
Argonne National Laboratory-East	Morocco	5
Argonne National Laboratory-East	Nepal	11
Argonne National Laboratory-East	Netherlands	41
Argonne National Laboratory-East	Netherlands Antilles	1
Argonne National Laboratory-East	New Zealand	20
Argonne National Laboratory-East	Nigeria	3
Argonne National Laboratory-East	Norway	6
Argonne National Laboratory-East	Pakistan	13
Argonne National Laboratory-East	Panama	1
Argonne National Laboratory-East	Peru	10
Argonne National Laboratory-East	Philippines	5
Argonne National Laboratory-East	Poland	72
Argonne National Laboratory-East	Portugal	13
Argonne National Laboratory-East	Romania	38
Argonne National Laboratory-East	Russia	162
Argonne National Laboratory-East	Saint Vincent and the Grenadines	1
Argonne National Laboratory-East	Saudi Arabia	2
Argonne National Laboratory-East	Serbia, Republic of	5
Argonne National Laboratory-East	Serbia-Montenegro	13
Argonne National Laboratory-East	Singapore	9
Argonne National Laboratory-East	Slovakia	9
Argonne National Laboratory-East	Slovenia	10
Argonne National Laboratory-East	South Africa	3
Argonne National Laboratory-East	Spain	64
Argonne National Laboratory-East	Sri Lanka	14
Argonne National Laboratory-East	Sweden	23
Argonne National Laboratory-East	Switzerland	26
Argonne National Laboratory-East	Taiwan	84
Argonne National Laboratory-East	Tanzania	2
Argonne National Laboratory-East	Thailand	11
Argonne National Laboratory-East	Tunisia	2
Argonne National Laboratory-East	Turkey	50
Argonne National Laboratory-East	Ukraine	36
Argonne National Laboratory-East	United Kingdom	303
Argonne National Laboratory-East	Uruguay	3
Argonne National Laboratory-East	Uzbekistan	7
Argonne National Laboratory-East	Venezuela	10
Argonne National Laboratory-East	Vietnam	10
Argonne National Laboratory-East	Yugoslavia, Federal Republic of	1
Argonne National Laboratory-East	Zimbabwe	2
Bayou Choctow Site, LA - SPRO	Canada	1
Bechtel National Incorporated	Argentina	1
Bechtel National Incorporated	Australia	2
Bechtel National Incorporated	Austria	1
Bechtel National Incorporated	Bangladesh	2
Bechtel National Incorporated	Bolivia	1
Bechtel National Incorporated	Bosnia-Herzegovina	1
Bechtel National Incorporated	Bulgaria	1

Bechtel National Incorporated	Canada	42
Bechtel National Incorporated	Chile	4
Bechtel National Incorporated	Croatia	1
Bechtel National Incorporated	Egypt	1
Bechtel National Incorporated	El Salvador	1
Bechtel National Incorporated	Ethiopia	1
Bechtel National Incorporated	France	1
Bechtel National Incorporated	Hong Kong	1
Bechtel National Incorporated	India	5
Bechtel National Incorporated	Indonesia	2
Bechtel National Incorporated	Ireland	1
Bechtel National Incorporated	Italy	1
Bechtel National Incorporated	Jamaica	1
Bechtel National Incorporated	Jordan	3
Bechtel National Incorporated	Korea, South	1
Bechtel National Incorporated	Lebanon	1
Bechtel National Incorporated	Malaysia	2
Bechtel National Incorporated	Mexico	16
Bechtel National Incorporated	Nicaragua	1
Bechtel National Incorporated	Nigeria	2
Bechtel National Incorporated	Pakistan	2
Bechtel National Incorporated	Peru	3
Bechtel National Incorporated	Philippines	5
Bechtel National Incorporated	Samoa	1
Bechtel National Incorporated	Singapore	2
Bechtel National Incorporated	South Africa	1
Bechtel National Incorporated	Taiwan	2
Bechtel National Incorporated	Turkey	1
Bechtel National Incorporated	Ukraine	3
Bechtel National Incorporated	United Kingdom	38
Bechtel National Incorporated	Venezuela	2
Bechtel National Incorporated	Vietnam	1
Bechtel National Incorporated	Zambia	1
Big Hill Site,TX - SPRO	Canada	1
Bonneville Power Administration	Canada	6
Bonneville Power Administration	China, People's Republic Of	2
Bonneville Power Administration	Croatia	1
Bonneville Power Administration	El Salvador	1
Bonneville Power Administration	Fiji	3
Bonneville Power Administration	Germany(Unified)	3
Bonneville Power Administration	India	1
Bonneville Power Administration	Kazakhstan	1
Bonneville Power Administration	Mexico	4
Bonneville Power Administration	Nepal	1
Bonneville Power Administration	Netherlands	1
Bonneville Power Administration	Philippines	2
Bonneville Power Administration	Russia	1
Bonneville Power Administration	Thailand	1
Bonneville Power Administration	Ukraine	2
Bonneville Power Administration	United Kingdom	3
Brookhaven National Laboratory	Afghanistan	1
Brookhaven National Laboratory	Albania	3
Brookhaven National Laboratory	Algeria	2
Brookhaven National Laboratory	Argentina	22
Brookhaven National Laboratory	Armenia	6
Brookhaven National Laboratory	Australia	38
Brookhaven National Laboratory	Austria	22
Brookhaven National Laboratory	Azerbaijan	4
Brookhaven National Laboratory	Bangladesh	10
Brookhaven National Laboratory	Barbados	2
Brookhaven National Laboratory	Belarus	9
Brookhaven National Laboratory	Belgium	15
Brookhaven National Laboratory	Bhutan	1
Brookhaven National Laboratory	Bolivia	2
Brookhaven National Laboratory	Bosnia-Herzegovina	1
Brookhaven National Laboratory	Brazil	51
Brookhaven National Laboratory	Bulgaria	6
Brookhaven National Laboratory	Burma	1
Brookhaven National Laboratory	Cameroon	3
Brookhaven National Laboratory	Canada	256
Brookhaven National Laboratory	Chile	4
Brookhaven National Laboratory	China, People's Republic Of	1395
Brookhaven National Laboratory	Colombia	17
Brookhaven National Laboratory	Cote D'Ivoire(Ivory Coast)	2
Brookhaven National Laboratory	Croatia	18
Brookhaven National Laboratory	Cyprus	2
Brookhaven National Laboratory	Czech Republic	34
Brookhaven National Laboratory	Denmark	24
Brookhaven National Laboratory	Dominica	1
Brookhaven National Laboratory	Dominican Republic	2
Brookhaven National Laboratory	Ecuador	4
Brookhaven National Laboratory	Egypt	4
Brookhaven National Laboratory	El Salvador	3
Brookhaven National Laboratory	Eritrea	1
Brookhaven National Laboratory	Estonia	1
Brookhaven National Laboratory	Ethiopia	7
Brookhaven National Laboratory	Fiji	1
Brookhaven National Laboratory	Finland	7

Brookhaven National Laboratory	France	180
Brookhaven National Laboratory	French Polynesia	1
Brookhaven National Laboratory	Gambia	1
Brookhaven National Laboratory	Georgia	6
Brookhaven National Laboratory	Germany(Unified)	336
Brookhaven National Laboratory	Ghana	9
Brookhaven National Laboratory	Greece	38
Brookhaven National Laboratory	Guyana	2
Brookhaven National Laboratory	Haiti	1
Brookhaven National Laboratory	Honduras	1
Brookhaven National Laboratory	Hong Kong	22
Brookhaven National Laboratory	Hungary	28
Brookhaven National Laboratory	Iceland	3
Brookhaven National Laboratory	India	617
Brookhaven National Laboratory	Indonesia	5
Brookhaven National Laboratory	Iran	2
Brookhaven National Laboratory	Iraq	11
Brookhaven National Laboratory	Ireland	14
Brookhaven National Laboratory	Israel	81
Brookhaven National Laboratory	Italy	149
Brookhaven National Laboratory	Jamaica	15
Brookhaven National Laboratory	Japan	333
Brookhaven National Laboratory	Jordan	8
Brookhaven National Laboratory	Kazakhstan	2
Brookhaven National Laboratory	Kenya	3
Brookhaven National Laboratory	Korea, South	222
Brookhaven National Laboratory	Lebanon	6
Brookhaven National Laboratory	Lithuania	4
Brookhaven National Laboratory	Macedonia, The Former Yugoslav Republic of	1
Brookhaven National Laboratory	Madagascar	1
Brookhaven National Laboratory	Malaysia	10
Brookhaven National Laboratory	Mauritius	3
Brookhaven National Laboratory	Mexico	41
Brookhaven National Laboratory	Morocco	2
Brookhaven National Laboratory	Nepal	5
Brookhaven National Laboratory	Netherlands	47
Brookhaven National Laboratory	Netherlands Antilles	3
Brookhaven National Laboratory	New Zealand	17
Brookhaven National Laboratory	Nicaragua	1
Brookhaven National Laboratory	Nigeria	12
Brookhaven National Laboratory	Norway	10
Brookhaven National Laboratory	Pakistan	24
Brookhaven National Laboratory	Palestine	1
Brookhaven National Laboratory	Panama	1
Brookhaven National Laboratory	Peru	5
Brookhaven National Laboratory	Philippines	15
Brookhaven National Laboratory	Poland	69
Brookhaven National Laboratory	Portugal	23
Brookhaven National Laboratory	Romania	47
Brookhaven National Laboratory	Russia	389
Brookhaven National Laboratory	Saint Lucia	2
Brookhaven National Laboratory	San Marino	1
Brookhaven National Laboratory	Senegal	2
Brookhaven National Laboratory	Singapore	10
Brookhaven National Laboratory	Slovakia	10
Brookhaven National Laboratory	South Africa	10
Brookhaven National Laboratory	Spain	59
Brookhaven National Laboratory	Sri Lanka	31
Brookhaven National Laboratory	Suriname	2
Brookhaven National Laboratory	Sweden	39
Brookhaven National Laboratory	Switzerland	17
Brookhaven National Laboratory	Taiwan	107
Brookhaven National Laboratory	Tanzania	1
Brookhaven National Laboratory	Thailand	21
Brookhaven National Laboratory	Trinidad and Tobago	10
Brookhaven National Laboratory	Tunisia	1
Brookhaven National Laboratory	Turkey	63
Brookhaven National Laboratory	Ukraine	49
Brookhaven National Laboratory	United Kingdom	250
Brookhaven National Laboratory	Uruguay	2
Brookhaven National Laboratory	Uzbekistan	2
Brookhaven National Laboratory	Venezuela	6
Brookhaven National Laboratory	Vietnam	10
Brookhaven National Laboratory	Yugoslavia, Federal Republic of	30
Brookhaven National Laboratory	Zimbabwe	1
Bryan Mound Site, TX - SPRO	Canada	2
DOE/HQ Forrestal Building	Belgium	1
DOE/HQ Forrestal Building	Canada	4
DOE/HQ Forrestal Building	Colombia	3
DOE/HQ Forrestal Building	Denmark	1
DOE/HQ Forrestal Building	Dominican Republic	2
DOE/HQ Forrestal Building	El Salvador	20
DOE/HQ Forrestal Building	Guatemala	1
DOE/HQ Forrestal Building	Guyana	1
DOE/HQ Forrestal Building	Honduras	1
DOE/HQ Forrestal Building	India	3
DOE/HQ Forrestal Building	Italy	1
DOE/HQ Forrestal Building	Jamaica	1

DOE/HQ Forrestal Building	Mexico	1
DOE/HQ Forrestal Building	Nepal	1
DOE/HQ Forrestal Building	Nicaragua	1
DOE/HQ Forrestal Building	Nigeria	1
DOE/HQ Forrestal Building	Norway	1
DOE/HQ Forrestal Building	Trinidad and Tobago	1
DOE/HQ Forrestal Building	Turkey	1
DOE/HQ Forrestal Building	Ukraine	1
DOE/HQ Forrestal Building	United Kingdom	4
DOE/HQ Germantown, Maryland	Canada	3
DOE/HQ Germantown, Maryland	China, People's Republic Of	17
DOE/HQ Germantown, Maryland	Colombia	2
DOE/HQ Germantown, Maryland	El Salvador	3
DOE/HQ Germantown, Maryland	Germany(Unified)	3
DOE/HQ Germantown, Maryland	Korea, South	1
DOE/HQ Germantown, Maryland	Poland	1
DOE/HQ Germantown, Maryland	United Kingdom	2
East Tennessee Technology Park	Malaysia	1
East Tennessee Technology Park	United Kingdom	1
Fermi National Accelerator Laboratory	Argentina	14
Fermi National Accelerator Laboratory	Armenia	3
Fermi National Accelerator Laboratory	Australia	4
Fermi National Accelerator Laboratory	Austria	2
Fermi National Accelerator Laboratory	Azerbaijan	1
Fermi National Accelerator Laboratory	Bangladesh	2
Fermi National Accelerator Laboratory	Belarus	3
Fermi National Accelerator Laboratory	Belgium	1
Fermi National Accelerator Laboratory	Brazil	14
Fermi National Accelerator Laboratory	Bulgaria	6
Fermi National Accelerator Laboratory	Canada	27
Fermi National Accelerator Laboratory	Chile	1
Fermi National Accelerator Laboratory	China, People's Republic Of	61
Fermi National Accelerator Laboratory	Colombia	2
Fermi National Accelerator Laboratory	Croatia	1
Fermi National Accelerator Laboratory	Cyprus	2
Fermi National Accelerator Laboratory	Czech Republic	3
Fermi National Accelerator Laboratory	Denmark	3
Fermi National Accelerator Laboratory	Ecuador	2
Fermi National Accelerator Laboratory	Egypt	2
Fermi National Accelerator Laboratory	El Salvador	4
Fermi National Accelerator Laboratory	Estonia	1
Fermi National Accelerator Laboratory	Finland	2
Fermi National Accelerator Laboratory	France	18
Fermi National Accelerator Laboratory	Georgia	6
Fermi National Accelerator Laboratory	Germany(Unified)	45
Fermi National Accelerator Laboratory	Ghana	1
Fermi National Accelerator Laboratory	Gibraltar	1
Fermi National Accelerator Laboratory	Greece	13
Fermi National Accelerator Laboratory	Honduras	3
Fermi National Accelerator Laboratory	Hong Kong	2
Fermi National Accelerator Laboratory	Hungary	3
Fermi National Accelerator Laboratory	India	57
Fermi National Accelerator Laboratory	Indonesia	3
Fermi National Accelerator Laboratory	Israel	2
Fermi National Accelerator Laboratory	Italy	87
Fermi National Accelerator Laboratory	Japan	51
Fermi National Accelerator Laboratory	Jordan	2
Fermi National Accelerator Laboratory	Kazakhstan	3
Fermi National Accelerator Laboratory	Korea, South	39
Fermi National Accelerator Laboratory	Kuwait	1
Fermi National Accelerator Laboratory	Malaysia	1
Fermi National Accelerator Laboratory	Mexico	38
Fermi National Accelerator Laboratory	Moldova	1
Fermi National Accelerator Laboratory	Mongolia	1
Fermi National Accelerator Laboratory	Nepal	3
Fermi National Accelerator Laboratory	Netherlands	5
Fermi National Accelerator Laboratory	New Zealand	3
Fermi National Accelerator Laboratory	Pakistan	6
Fermi National Accelerator Laboratory	Paraguay	1
Fermi National Accelerator Laboratory	Peru	7
Fermi National Accelerator Laboratory	Philippines	1
Fermi National Accelerator Laboratory	Poland	6
Fermi National Accelerator Laboratory	Romania	8
Fermi National Accelerator Laboratory	Russia	116
Fermi National Accelerator Laboratory	Saint Lucia	1
Fermi National Accelerator Laboratory	Serbia, Republic of	1
Fermi National Accelerator Laboratory	Singapore	2
Fermi National Accelerator Laboratory	Slovakia	2
Fermi National Accelerator Laboratory	Slovenia	2
Fermi National Accelerator Laboratory	South Africa	1
Fermi National Accelerator Laboratory	Spain	17
Fermi National Accelerator Laboratory	Sri Lanka	1
Fermi National Accelerator Laboratory	Sweden	2
Fermi National Accelerator Laboratory	Switzerland	2
Fermi National Accelerator Laboratory	Taiwan	9
Fermi National Accelerator Laboratory	Tanzania	1
Fermi National Accelerator Laboratory	Turkey	18
Fermi National Accelerator Laboratory	Ukraine	8

Fermi National Accelerator Laboratory	United Kingdom	46
Fermi National Accelerator Laboratory	Uzbekistan	2
Fermi National Accelerator Laboratory	Venezuela	1
Fermi National Accelerator Laboratory	Vietnam	2
Fermi National Accelerator Laboratory	Yugoslavia, Federal Republic of	1
General Atomics	China, People's Republic Of	1
General Atomics	India	3
General Atomics	Japan	1
General Atomics	Korea, South	2
General Atomics	Russia	1
Hanford Site - Bechtel	Australia	2
Hanford Site - Bechtel	Canada	2
Hanford Site - Bechtel	Mexico	11
Hanford Site - Bechtel	Nigeria	1
Hanford Site - Bechtel	United Kingdom	2
Hanford Site - Bechtel	Vietnam	1
Hanford Site - Fluor Daniel	Australia	1
Hanford Site - Fluor Daniel	Canada	5
Hanford Site - Fluor Daniel	Egypt	1
Hanford Site - Fluor Daniel	France	2
Hanford Site - Fluor Daniel	Ireland	1
Hanford Site - Fluor Daniel	Japan	1
Hanford Site - Fluor Daniel	Mexico	3
Hanford Site - Fluor Daniel	Netherlands	1
Hanford Site - Fluor Daniel	Nigeria	2
Hanford Site - Fluor Daniel	Russia	1
Hanford Site - Fluor Daniel	United Kingdom	5
Hanford Tank Farms	Austria	1
Hanford Tank Farms	Brazil	1
Hanford Tank Farms	Canada	4
Hanford Tank Farms	France	3
Hanford Tank Farms	Japan	1
Hanford Tank Farms	Korea, South	2
Hanford Tank Farms	Nigeria	1
Hanford Tank Farms	Russia	2
Hanford Tank Farms	Ukraine	1
Hanford Tank Farms	United Kingdom	6
Idaho National Engineering Laboratory	Argentina	2
Idaho National Engineering Laboratory	Canada	6
Idaho National Engineering Laboratory	China, People's Republic Of	4
Idaho National Engineering Laboratory	Finland	1
Idaho National Engineering Laboratory	France	4
Idaho National Engineering Laboratory	India	4
Idaho National Engineering Laboratory	Italy	5
Idaho National Engineering Laboratory	Japan	1
Idaho National Engineering Laboratory	Jordan	1
Idaho National Engineering Laboratory	Korea, South	4
Idaho National Engineering Laboratory	Netherlands	2
Idaho National Engineering Laboratory	Romania	2
Idaho National Engineering Laboratory	Russia	3
Idaho National Engineering Laboratory	United Kingdom	4
Lawrence Berkeley Laboratory	Algeria	2
Lawrence Berkeley Laboratory	Australia	3
Lawrence Berkeley Laboratory	Azerbaijan	1
Lawrence Berkeley Laboratory	Belarus	4
Lawrence Berkeley Laboratory	Canada	13
Lawrence Berkeley Laboratory	China, People's Republic Of	358
Lawrence Berkeley Laboratory	Czech Republic	1
Lawrence Berkeley Laboratory	France	4
Lawrence Berkeley Laboratory	Germany(Unified)	3
Lawrence Berkeley Laboratory	Hong Kong	5
Lawrence Berkeley Laboratory	India	163
Lawrence Berkeley Laboratory	Iran	4
Lawrence Berkeley Laboratory	Iraq	1
Lawrence Berkeley Laboratory	Israel	21
Lawrence Berkeley Laboratory	Japan	1
Lawrence Berkeley Laboratory	Kazakhstan	1
Lawrence Berkeley Laboratory	Korea, South	1
Lawrence Berkeley Laboratory	Moldova	2
Lawrence Berkeley Laboratory	New Zealand	1
Lawrence Berkeley Laboratory	Nigeria	2
Lawrence Berkeley Laboratory	Norway	1
Lawrence Berkeley Laboratory	Pakistan	3
Lawrence Berkeley Laboratory	Poland	1
Lawrence Berkeley Laboratory	Russia	58
Lawrence Berkeley Laboratory	Singapore	1
Lawrence Berkeley Laboratory	South Africa	1
Lawrence Berkeley Laboratory	Sweden	2
Lawrence Berkeley Laboratory	Taiwan	46
Lawrence Berkeley Laboratory	Turkey	1
Lawrence Berkeley Laboratory	Ukraine	8
Lawrence Berkeley Laboratory	United Kingdom	6
Lawrence Livermore National Laboratory	Argentina	34
Lawrence Livermore National Laboratory	Australia	36
Lawrence Livermore National Laboratory	Austria	18
Lawrence Livermore National Laboratory	Belgium	44
Lawrence Livermore National Laboratory	Belize	2
Lawrence Livermore National Laboratory	Benin	3

Lawrence Livermore National Laboratory	Brazil	17
Lawrence Livermore National Laboratory	Bulgaria	19
Lawrence Livermore National Laboratory	Canada	153
Lawrence Livermore National Laboratory	Chile	5
Lawrence Livermore National Laboratory	China, People's Republic Of	93
Lawrence Livermore National Laboratory	Costa Rica	2
Lawrence Livermore National Laboratory	Croatia	7
Lawrence Livermore National Laboratory	Cyprus	2
Lawrence Livermore National Laboratory	Czech Republic	5
Lawrence Livermore National Laboratory	Denmark	15
Lawrence Livermore National Laboratory	Dominican Republic	4
Lawrence Livermore National Laboratory	Egypt	8
Lawrence Livermore National Laboratory	Finland	3
Lawrence Livermore National Laboratory	France	112
Lawrence Livermore National Laboratory	Germany(Unified)	210
Lawrence Livermore National Laboratory	Ghana	2
Lawrence Livermore National Laboratory	Greece	6
Lawrence Livermore National Laboratory	Hungary	7
Lawrence Livermore National Laboratory	Iceland	4
Lawrence Livermore National Laboratory	India	102
Lawrence Livermore National Laboratory	Ireland	23
Lawrence Livermore National Laboratory	Israel	37
Lawrence Livermore National Laboratory	Italy	82
Lawrence Livermore National Laboratory	Japan	29
Lawrence Livermore National Laboratory	Korea, South	97
Lawrence Livermore National Laboratory	Lebanon	16
Lawrence Livermore National Laboratory	Macau	5
Lawrence Livermore National Laboratory	Macedonia, The Former Yugoslav Republic of	4
Lawrence Livermore National Laboratory	Malaysia	2
Lawrence Livermore National Laboratory	Mexico	5
Lawrence Livermore National Laboratory	Mongolia	3
Lawrence Livermore National Laboratory	Montenegro	3
Lawrence Livermore National Laboratory	Netherlands	6
Lawrence Livermore National Laboratory	New Zealand	9
Lawrence Livermore National Laboratory	Nigeria	3
Lawrence Livermore National Laboratory	Pakistan	2
Lawrence Livermore National Laboratory	Poland	17
Lawrence Livermore National Laboratory	Portugal	5
Lawrence Livermore National Laboratory	Romania	14
Lawrence Livermore National Laboratory	Russia	40
Lawrence Livermore National Laboratory	Serbia-Montenegro	2
Lawrence Livermore National Laboratory	South Africa	15
Lawrence Livermore National Laboratory	Spain	30
Lawrence Livermore National Laboratory	Sweden	59
Lawrence Livermore National Laboratory	Switzerland	12
Lawrence Livermore National Laboratory	Taiwan	10
Lawrence Livermore National Laboratory	Thailand	2
Lawrence Livermore National Laboratory	Turkey	25
Lawrence Livermore National Laboratory	Uganda	2
Lawrence Livermore National Laboratory	United Kingdom	98
Lawrence Livermore National Laboratory	Vietnam	3
Los Alamos National Laboratory	Albania	1
Los Alamos National Laboratory	Algeria	1
Los Alamos National Laboratory	Argentina	5
Los Alamos National Laboratory	Australia	5
Los Alamos National Laboratory	Austria	4
Los Alamos National Laboratory	Bangladesh	1
Los Alamos National Laboratory	Belarus	4
Los Alamos National Laboratory	Belgium	2
Los Alamos National Laboratory	Brazil	1
Los Alamos National Laboratory	Bulgaria	1
Los Alamos National Laboratory	Burma	1
Los Alamos National Laboratory	Canada	13
Los Alamos National Laboratory	China, People's Republic Of	115
Los Alamos National Laboratory	Colombia	1
Los Alamos National Laboratory	Costa Rica	1
Los Alamos National Laboratory	Croatia	1
Los Alamos National Laboratory	Denmark	1
Los Alamos National Laboratory	Egypt	2
Los Alamos National Laboratory	El Salvador	3
Los Alamos National Laboratory	France	3
Los Alamos National Laboratory	Georgia	1
Los Alamos National Laboratory	Germany(Unified)	24
Los Alamos National Laboratory	Greece	1
Los Alamos National Laboratory	Honduras	1
Los Alamos National Laboratory	India	64
Los Alamos National Laboratory	Indonesia	1
Los Alamos National Laboratory	Israel	8
Los Alamos National Laboratory	Italy	4
Los Alamos National Laboratory	Japan	7
Los Alamos National Laboratory	Jordan	3
Los Alamos National Laboratory	Korea, South	7
Los Alamos National Laboratory	Lebanon	1
Los Alamos National Laboratory	Mexico	17
Los Alamos National Laboratory	Netherlands	3
Los Alamos National Laboratory	Netherlands Antilles	1
Los Alamos National Laboratory	New Zealand	1
Los Alamos National Laboratory	Poland	3

Los Alamos National Laboratory	Romania	6
Los Alamos National Laboratory	Russia	40
Los Alamos National Laboratory	Serbia, Republic of	1
Los Alamos National Laboratory	Slovakia	1
Los Alamos National Laboratory	South Africa	1
Los Alamos National Laboratory	Spain	1
Los Alamos National Laboratory	Sri Lanka	2
Los Alamos National Laboratory	Sweden	6
Los Alamos National Laboratory	Switzerland	2
Los Alamos National Laboratory	Taiwan	7
Los Alamos National Laboratory	Turkey	5
Los Alamos National Laboratory	Turkmenistan	1
Los Alamos National Laboratory	Ukraine	6
Los Alamos National Laboratory	United Kingdom	15
Los Alamos National Laboratory	Venezuela	2
Los Alamos National Laboratory	Yugoslavia, Federal Republic of	1
MOX Project Office - Aiken, SC	France	1
National Energy Technology Laboratory	Algeria	1
National Energy Technology Laboratory	Argentina	1
National Energy Technology Laboratory	Armenia	1
National Energy Technology Laboratory	Brazil	1
National Energy Technology Laboratory	Canada	6
National Energy Technology Laboratory	China, People's Republic Of	38
National Energy Technology Laboratory	Colombia	1
National Energy Technology Laboratory	France	3
National Energy Technology Laboratory	Georgia	1
National Energy Technology Laboratory	Germany(Unified)	1
National Energy Technology Laboratory	Greece	1
National Energy Technology Laboratory	Hong Kong	1
National Energy Technology Laboratory	India	31
National Energy Technology Laboratory	Israel	1
National Energy Technology Laboratory	Italy	1
National Energy Technology Laboratory	Japan	3
National Energy Technology Laboratory	Korea, South	5
National Energy Technology Laboratory	Mexico	13
National Energy Technology Laboratory	Nepal	1
National Energy Technology Laboratory	Nigeria	1
National Energy Technology Laboratory	Philippines	1
National Energy Technology Laboratory	Poland	1
National Energy Technology Laboratory	Russia	4
National Energy Technology Laboratory	Spain	1
National Energy Technology Laboratory	Taiwan	1
National Energy Technology Laboratory	Thailand	1
National Energy Technology Laboratory	Turkey	6
National Energy Technology Laboratory	Uganda	1
National Energy Technology Laboratory	United Kingdom	2
National Energy Technology Laboratory	Venezuela	1
National Energy Technology Laboratory	Zambia	1
National Renewable Energy Laboratory	Algeria	1
National Renewable Energy Laboratory	Australia	1
National Renewable Energy Laboratory	Bulgaria	1
National Renewable Energy Laboratory	Canada	1
National Renewable Energy Laboratory	China, People's Republic Of	12
National Renewable Energy Laboratory	Colombia	1
National Renewable Energy Laboratory	Finland	2
National Renewable Energy Laboratory	India	7
National Renewable Energy Laboratory	Ireland	1
National Renewable Energy Laboratory	Korea, South	3
National Renewable Energy Laboratory	Lebanon	1
National Renewable Energy Laboratory	Mexico	18
National Renewable Energy Laboratory	Netherlands	2
National Renewable Energy Laboratory	Peru	1
National Renewable Energy Laboratory	Poland	1
National Renewable Energy Laboratory	Romania	1
National Renewable Energy Laboratory	Spain	1
National Renewable Energy Laboratory	Taiwan	1
National Renewable Energy Laboratory	United Arab Emirates	1
National Renewable Energy Laboratory	United Kingdom	4
National Renewable Energy Laboratory	Venezuela	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Canada	16
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Chile	3
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	China, People's Republic Of	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	France	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	India	5
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Israel	8
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Italy	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Mexico	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Netherlands	3

Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	New Zealand	2
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Russia	6
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Singapore	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Switzerland	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Thailand	1
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	United Kingdom	15
Naval Petroleum & Oil Shale Reserves(FE),Casper,WY	Venezuela	1
Nevada Operations Office	China, People's Republic Of	1
Nevada Operations Office	Egypt	1
Nevada Test Site	Canada	22
Nevada Test Site	China, People's Republic Of	2
Nevada Test Site	India	2
Nevada Test Site	Japan	1
Nevada Test Site	United Kingdom	3
New Brunswick Laboratory	Germany(Unified)	2
North Las Vegas Facility	Canada	3
North Las Vegas Facility	France	8
North Las Vegas Facility	Germany(Unified)	4
North Las Vegas Facility	Russia	2
North Las Vegas Facility	Switzerland	1
North Las Vegas Facility	United Kingdom	3
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	Canada	1
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	China, People's Republic Of	6
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	Germany(Unified)	1
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	India	1
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	Korea, South	1
Nuclear Weapons Prod Facility, Oak Ridge, Y-12	United Kingdom	1
NV at Livermore, CA	Austria	1
NV at Livermore, CA	Germany(Unified)	1
NV at Livermore, CA	Italy	1
NV at Livermore, CA	Russia	1
NV at Livermore, CA	United Kingdom	3
NV at Los Alamos, NM	Austria	1
Oak Ridge Associated Universities	Canada	4
Oak Ridge Associated Universities	Liberia	1
Oak Ridge Associated Universities	Slovenia	5
Oak Ridge National Laboratory	Argentina	10
Oak Ridge National Laboratory	Australia	27
Oak Ridge National Laboratory	Austria	8
Oak Ridge National Laboratory	Bahamas	1
Oak Ridge National Laboratory	Bangladesh	10
Oak Ridge National Laboratory	Barbados	1
Oak Ridge National Laboratory	Belarus	1
Oak Ridge National Laboratory	Belgium	11
Oak Ridge National Laboratory	Bolivia	2
Oak Ridge National Laboratory	Brazil	20
Oak Ridge National Laboratory	Brunei	1
Oak Ridge National Laboratory	Bulgaria	10
Oak Ridge National Laboratory	Cameroon	1
Oak Ridge National Laboratory	Canada	98
Oak Ridge National Laboratory	China, People's Republic Of	419
Oak Ridge National Laboratory	Colombia	10
Oak Ridge National Laboratory	Croatia	4
Oak Ridge National Laboratory	Cyprus	2
Oak Ridge National Laboratory	Czech Republic	7
Oak Ridge National Laboratory	Denmark	6
Oak Ridge National Laboratory	Ecuador	1
Oak Ridge National Laboratory	Egypt	6
Oak Ridge National Laboratory	El Salvador	3
Oak Ridge National Laboratory	Ethiopia	5
Oak Ridge National Laboratory	Finland	5
Oak Ridge National Laboratory	France	50
Oak Ridge National Laboratory	Georgia	2
Oak Ridge National Laboratory	Germany(Unified)	151
Oak Ridge National Laboratory	Ghana	3
Oak Ridge National Laboratory	Greece	9
Oak Ridge National Laboratory	Guatemala	1
Oak Ridge National Laboratory	Haiti	2
Oak Ridge National Laboratory	Hong Kong	5
Oak Ridge National Laboratory	Hungary	12
Oak Ridge National Laboratory	India	232
Oak Ridge National Laboratory	Indonesia	10
Oak Ridge National Laboratory	Ireland	7
Oak Ridge National Laboratory	Israel	11
Oak Ridge National Laboratory	Italy	47

Oak Ridge National Laboratory	Japan	74
Oak Ridge National Laboratory	Jordan	4
Oak Ridge National Laboratory	Kazakhstan	1
Oak Ridge National Laboratory	Kenya	4
Oak Ridge National Laboratory	Korea, South	99
Oak Ridge National Laboratory	Latvia	1
Oak Ridge National Laboratory	Lebanon	6
Oak Ridge National Laboratory	Liberia	1
Oak Ridge National Laboratory	Luxembourg	1
Oak Ridge National Laboratory	Macedonia, The Former Yugoslav Republic of	1
Oak Ridge National Laboratory	Malaysia	7
Oak Ridge National Laboratory	Mexico	15
Oak Ridge National Laboratory	Montenegro	1
Oak Ridge National Laboratory	Nepal	10
Oak Ridge National Laboratory	Netherlands	21
Oak Ridge National Laboratory	New Zealand	5
Oak Ridge National Laboratory	Nigeria	6
Oak Ridge National Laboratory	Norway	9
Oak Ridge National Laboratory	Pakistan	5
Oak Ridge National Laboratory	Paraguay	1
Oak Ridge National Laboratory	Peru	5
Oak Ridge National Laboratory	Philippines	5
Oak Ridge National Laboratory	Poland	25
Oak Ridge National Laboratory	Portugal	4
Oak Ridge National Laboratory	Romania	23
Oak Ridge National Laboratory	Russia	95
Oak Ridge National Laboratory	Saint Lucia	1
Oak Ridge National Laboratory	Senegal	1
Oak Ridge National Laboratory	Singapore	2
Oak Ridge National Laboratory	Slovakia	6
Oak Ridge National Laboratory	Slovenia	1
Oak Ridge National Laboratory	South Africa	2
Oak Ridge National Laboratory	Spain	21
Oak Ridge National Laboratory	Sri Lanka	8
Oak Ridge National Laboratory	Sweden	10
Oak Ridge National Laboratory	Switzerland	12
Oak Ridge National Laboratory	Taiwan	23
Oak Ridge National Laboratory	Thailand	9
Oak Ridge National Laboratory	Trinidad and Tobago	1
Oak Ridge National Laboratory	Turkey	27
Oak Ridge National Laboratory	Ukraine	17
Oak Ridge National Laboratory	United Kingdom	145
Oak Ridge National Laboratory	Uruguay	3
Oak Ridge National Laboratory	Uzbekistan	3
Oak Ridge National Laboratory	Venezuela	7
Oak Ridge National Laboratory	Vietnam	3
Oak Ridge National Laboratory	Yugoslavia, Federal Republic of	1
Oak Ridge National Laboratory	Zimbabwe	1
Office of River Protection	Canada	1
Office of River Protection	Nigeria	1
Pacific Northwest National Laboratory	Albania	2
Pacific Northwest National Laboratory	Algeria	2
Pacific Northwest National Laboratory	Argentina	2
Pacific Northwest National Laboratory	Australia	12
Pacific Northwest National Laboratory	Austria	2
Pacific Northwest National Laboratory	Bangladesh	5
Pacific Northwest National Laboratory	Belgium	6
Pacific Northwest National Laboratory	Belize	1
Pacific Northwest National Laboratory	Brazil	9
Pacific Northwest National Laboratory	Bulgaria	8
Pacific Northwest National Laboratory	Canada	49
Pacific Northwest National Laboratory	China, People's Republic Of	275
Pacific Northwest National Laboratory	Colombia	1
Pacific Northwest National Laboratory	Costa Rica	1
Pacific Northwest National Laboratory	Cote D'Ivoire(Ivory Coast)	1
Pacific Northwest National Laboratory	Czech Republic	8
Pacific Northwest National Laboratory	Denmark	2
Pacific Northwest National Laboratory	Egypt	5
Pacific Northwest National Laboratory	El Salvador	2
Pacific Northwest National Laboratory	Eritrea	2
Pacific Northwest National Laboratory	Fiji	3
Pacific Northwest National Laboratory	France	13
Pacific Northwest National Laboratory	Germany(Unified)	16
Pacific Northwest National Laboratory	Ghana	2
Pacific Northwest National Laboratory	Greece	6
Pacific Northwest National Laboratory	Guatemala	1
Pacific Northwest National Laboratory	Hungary	2
Pacific Northwest National Laboratory	Iceland	3
Pacific Northwest National Laboratory	India	130
Pacific Northwest National Laboratory	Ireland	6
Pacific Northwest National Laboratory	Israel	5
Pacific Northwest National Laboratory	Italy	15
Pacific Northwest National Laboratory	Japan	12
Pacific Northwest National Laboratory	Jordan	4
Pacific Northwest National Laboratory	Kazakhstan	2
Pacific Northwest National Laboratory	Kenya	2
Pacific Northwest National Laboratory	Korea, South	40
Pacific Northwest National Laboratory	Kyrgyzstan (Kyrgyz Republic)	1

Pacific Northwest National Laboratory	Latvia	2
Pacific Northwest National Laboratory	Lebanon	1
Pacific Northwest National Laboratory	Macedonia, The Former Yugoslav Republic of	1
Pacific Northwest National Laboratory	Mexico	6
Pacific Northwest National Laboratory	Moldova	1
Pacific Northwest National Laboratory	Morocco	3
Pacific Northwest National Laboratory	Nepal	1
Pacific Northwest National Laboratory	Netherlands	9
Pacific Northwest National Laboratory	Netherlands Antilles	3
Pacific Northwest National Laboratory	Nigeria	8
Pacific Northwest National Laboratory	Norway	3
Pacific Northwest National Laboratory	Pakistan	2
Pacific Northwest National Laboratory	Poland	15
Pacific Northwest National Laboratory	Romania	9
Pacific Northwest National Laboratory	Russia	91
Pacific Northwest National Laboratory	South Africa	2
Pacific Northwest National Laboratory	Spain	6
Pacific Northwest National Laboratory	Sri Lanka	18
Pacific Northwest National Laboratory	Sweden	8
Pacific Northwest National Laboratory	Switzerland	5
Pacific Northwest National Laboratory	Taiwan	17
Pacific Northwest National Laboratory	Thailand	7
Pacific Northwest National Laboratory	Trinidad and Tobago	3
Pacific Northwest National Laboratory	Turkey	3
Pacific Northwest National Laboratory	Ukraine	17
Pacific Northwest National Laboratory	United Kingdom	65
Pacific Northwest National Laboratory	Uzbekistan	1
Pacific Northwest National Laboratory	Yugoslavia, Federal Republic of	2
Pacific Northwest National Laboratory	Zambia	2
Portsmouth Gaseous Diffusion Plant	Netherlands	2
Princeton Plasma Physics Laboratory	Canada	1
Princeton Plasma Physics Laboratory	China, People's Republic Of	17
Princeton Plasma Physics Laboratory	India	3
Princeton Plasma Physics Laboratory	Israel	1
Princeton Plasma Physics Laboratory	Russia	11
Remote Sensing Laboratory, Nellis AFB	Canada	1
Richland Operations Office	Canada	2
Richland Operations Office	France	1
Richland Operations Office	Ireland	1
Richland Operations Office	Japan	1
Richland Operations Office	Nigeria	1
Richland Operations Office	United Kingdom	3
RSL at Andrews Air Force Base	Germany(Unified)	1
Sandia National Laboratories, Albuquerque	Argentina	3
Sandia National Laboratories, Albuquerque	Australia	6
Sandia National Laboratories, Albuquerque	Austria	3
Sandia National Laboratories, Albuquerque	Bangladesh	3
Sandia National Laboratories, Albuquerque	Belarus	12
Sandia National Laboratories, Albuquerque	Belgium	1
Sandia National Laboratories, Albuquerque	Brazil	2
Sandia National Laboratories, Albuquerque	Bulgaria	1
Sandia National Laboratories, Albuquerque	Canada	27
Sandia National Laboratories, Albuquerque	China, People's Republic Of	73
Sandia National Laboratories, Albuquerque	Colombia	1
Sandia National Laboratories, Albuquerque	Cyprus	1
Sandia National Laboratories, Albuquerque	Denmark	1
Sandia National Laboratories, Albuquerque	Egypt	4
Sandia National Laboratories, Albuquerque	Ethiopia	2
Sandia National Laboratories, Albuquerque	Finland	2
Sandia National Laboratories, Albuquerque	France	20
Sandia National Laboratories, Albuquerque	Germany(Unified)	15
Sandia National Laboratories, Albuquerque	Greece	8
Sandia National Laboratories, Albuquerque	Iceland	1
Sandia National Laboratories, Albuquerque	India	48
Sandia National Laboratories, Albuquerque	Iraq	2

Sandia National Laboratories, Albuquerque	Ireland	3
Sandia National Laboratories, Albuquerque	Israel	6
Sandia National Laboratories, Albuquerque	Italy	7
Sandia National Laboratories, Albuquerque	Jamaica	1
Sandia National Laboratories, Albuquerque	Japan	16
Sandia National Laboratories, Albuquerque	Jordan	8
Sandia National Laboratories, Albuquerque	Korea, South	11
Sandia National Laboratories, Albuquerque	Macedonia, The Former Yugoslav Republic of	2
Sandia National Laboratories, Albuquerque	Mexico	4
Sandia National Laboratories, Albuquerque	Morocco	1
Sandia National Laboratories, Albuquerque	Nepal	2
Sandia National Laboratories, Albuquerque	Netherlands	9
Sandia National Laboratories, Albuquerque	Norway	1
Sandia National Laboratories, Albuquerque	Poland	1
Sandia National Laboratories, Albuquerque	Portugal	1
Sandia National Laboratories, Albuquerque	Romania	1
Sandia National Laboratories, Albuquerque	Russia	34
Sandia National Laboratories, Albuquerque	Spain	4
Sandia National Laboratories, Albuquerque	Switzerland	2
Sandia National Laboratories, Albuquerque	Taiwan	2
Sandia National Laboratories, Albuquerque	Tanzania	3
Sandia National Laboratories, Albuquerque	Thailand	1
Sandia National Laboratories, Albuquerque	Turkey	5
Sandia National Laboratories, Albuquerque	Ukraine	2
Sandia National Laboratories, Albuquerque	United Kingdom	28
Sandia National Laboratories, Albuquerque	Uruguay	2
Sandia National Laboratories, Livermore, CA	Armenia	2
Sandia National Laboratories, Livermore, CA	Australia	11
Sandia National Laboratories, Livermore, CA	Bangladesh	2
Sandia National Laboratories, Livermore, CA	Brazil	1
Sandia National Laboratories, Livermore, CA	Canada	6
Sandia National Laboratories, Livermore, CA	China, People's Republic Of	37
Sandia National Laboratories, Livermore, CA	Denmark	4
Sandia National Laboratories, Livermore, CA	France	12
Sandia National Laboratories, Livermore, CA	Germany(Unified)	20
Sandia National Laboratories, Livermore, CA	Greece	2
Sandia National Laboratories, Livermore, CA	Hungary	1
Sandia National Laboratories, Livermore, CA	Iceland	4
Sandia National Laboratories, Livermore, CA	India	33
Sandia National Laboratories, Livermore, CA	Ireland	3
Sandia National Laboratories, Livermore, CA	Italy	4
Sandia National Laboratories, Livermore, CA	Japan	1
Sandia National Laboratories, Livermore, CA	Korea, South	15
Sandia National Laboratories, Livermore, CA	Malaysia	1

Sandia National Laboratories, Livermore, CA	Mexico	3
Sandia National Laboratories, Livermore, CA	Moldova	4
Sandia National Laboratories, Livermore, CA	Netherlands	3
Sandia National Laboratories, Livermore, CA	New Zealand	1
Sandia National Laboratories, Livermore, CA	Norway	2
Sandia National Laboratories, Livermore, CA	Peru	1
Sandia National Laboratories, Livermore, CA	Philippines	2
Sandia National Laboratories, Livermore, CA	Romania	13
Sandia National Laboratories, Livermore, CA	Russia	11
Sandia National Laboratories, Livermore, CA	Senegal	1
Sandia National Laboratories, Livermore, CA	Spain	15
Sandia National Laboratories, Livermore, CA	Sri Lanka	1
Sandia National Laboratories, Livermore, CA	Sweden	3
Sandia National Laboratories, Livermore, CA	Switzerland	3
Sandia National Laboratories, Livermore, CA	Taiwan	4
Sandia National Laboratories, Livermore, CA	Turkey	4
Sandia National Laboratories, Livermore, CA	United Kingdom	14
Sandia National Laboratories, Livermore, CA	Zimbabwe	1
Santa Barbara Office - Special Technologies Lab	Austria	1
Santa Barbara Office - Special Technologies Lab	Romania	1
Savannah River Operations Office	Argentina	1
Savannah River Operations Office	Australia	1
Savannah River Operations Office	Bangladesh	1
Savannah River Operations Office	Brazil	1
Savannah River Operations Office	Canada	13
Savannah River Operations Office	China, People's Republic Of	9
Savannah River Operations Office	Dominican Republic	1
Savannah River Operations Office	Egypt	1
Savannah River Operations Office	Ethiopia	1
Savannah River Operations Office	France	62
Savannah River Operations Office	Germany(Unified)	1
Savannah River Operations Office	Hungary	1
Savannah River Operations Office	India	6
Savannah River Operations Office	Indonesia	1
Savannah River Operations Office	Italy	1
Savannah River Operations Office	Jamaica	1
Savannah River Operations Office	Japan	3
Savannah River Operations Office	Jordan	2
Savannah River Operations Office	Korea, South	6
Savannah River Operations Office	Lebanon	1
Savannah River Operations Office	Nepal	1
Savannah River Operations Office	Nicaragua	1
Savannah River Operations Office	Nigeria	1
Savannah River Operations Office	Norway	1
Savannah River Operations Office	Poland	1
Savannah River Operations Office	Romania	1
Savannah River Operations Office	Russia	1
Savannah River Operations Office	Slovakia	1
Savannah River Operations Office	Spain	4
Savannah River Operations Office	Thailand	2
Savannah River Operations Office	Ukraine	1
Savannah River Operations Office	United Kingdom	14
Savannah River Operations Office	Vietnam	1
Stanford Linear Accelerator Center	Albania	1
Stanford Linear Accelerator Center	American Samoa	2
Stanford Linear Accelerator Center	Australia	1
Stanford Linear Accelerator Center	Canada	5
Stanford Linear Accelerator Center	China, People's Republic Of	93
Stanford Linear Accelerator Center	France	1
Stanford Linear Accelerator Center	Hong Kong	1
Stanford Linear Accelerator Center	India	41
Stanford Linear Accelerator Center	Iran	5
Stanford Linear Accelerator Center	Israel	4
Stanford Linear Accelerator Center	Italy	1
Stanford Linear Accelerator Center	Libya	1
Stanford Linear Accelerator Center	Mexico	4
Stanford Linear Accelerator Center	Pakistan	3
Stanford Linear Accelerator Center	Russia	20

Stanford Linear Accelerator Center	Taiwan	21
Stanford Linear Accelerator Center	Turkmenistan	1
Stanford Linear Accelerator Center	Ukraine	1
Stanford Linear Accelerator Center	United Kingdom	2
Strategic Petroleum Reserve Project Office	Canada	2
Thomas Jefferson National Accelerator Facility	Argentina	1
Thomas Jefferson National Accelerator Facility	Armenia	14
Thomas Jefferson National Accelerator Facility	Australia	3
Thomas Jefferson National Accelerator Facility	Bahamas	1
Thomas Jefferson National Accelerator Facility	Bolivia	1
Thomas Jefferson National Accelerator Facility	Bulgaria	2
Thomas Jefferson National Accelerator Facility	Canada	7
Thomas Jefferson National Accelerator Facility	China, People's Republic Of	40
Thomas Jefferson National Accelerator Facility	Colombia	1
Thomas Jefferson National Accelerator Facility	Croatia	1
Thomas Jefferson National Accelerator Facility	France	11
Thomas Jefferson National Accelerator Facility	Germany(Unified)	22
Thomas Jefferson National Accelerator Facility	Greece	2
Thomas Jefferson National Accelerator Facility	Hungary	1
Thomas Jefferson National Accelerator Facility	India	18
Thomas Jefferson National Accelerator Facility	Iran	3
Thomas Jefferson National Accelerator Facility	Israel	1
Thomas Jefferson National Accelerator Facility	Italy	6
Thomas Jefferson National Accelerator Facility	Japan	7
Thomas Jefferson National Accelerator Facility	Jordan	1
Thomas Jefferson National Accelerator Facility	Korea, South	4
Thomas Jefferson National Accelerator Facility	Mexico	2
Thomas Jefferson National Accelerator Facility	Morocco	2
Thomas Jefferson National Accelerator Facility	Nepal	3
Thomas Jefferson National Accelerator Facility	Netherlands	4
Thomas Jefferson National Accelerator Facility	Poland	2
Thomas Jefferson National Accelerator Facility	Portugal	1
Thomas Jefferson National Accelerator Facility	Romania	3
Thomas Jefferson National Accelerator Facility	Russia	23
Thomas Jefferson National Accelerator Facility	Spain	1
Thomas Jefferson National Accelerator Facility	Sri Lanka	3
Thomas Jefferson National Accelerator Facility	Sweden	1
Thomas Jefferson National Accelerator Facility	Switzerland	1
Thomas Jefferson National Accelerator Facility	Thailand	2
Thomas Jefferson National Accelerator Facility	Trinidad and Tobago	1
Thomas Jefferson National Accelerator Facility	Turkey	5
Thomas Jefferson National Accelerator Facility	Turkmenistan	1
Thomas Jefferson National Accelerator Facility	Ukraine	4
Thomas Jefferson National Accelerator Facility	United Kingdom	10
Thomas Jefferson National Accelerator Facility	Uzbekistan	2
TRU Waste Processing Facility, Oak Ridge	Canada	3

TRU Waste Processing Facility, Oak Ridge	United Kingdom	4
University of Rochester	Australia	1
University of Rochester	Austria	2
University of Rochester	Bangladesh	1
University of Rochester	Canada	2
University of Rochester	China, People's Republic Of	22
University of Rochester	Colombia	1
University of Rochester	France	5
University of Rochester	Germany(Unified)	5
University of Rochester	Ireland	1
University of Rochester	Israel	3
University of Rochester	Italy	1
University of Rochester	Japan	2
University of Rochester	Korea, South	3
University of Rochester	Netherlands	1
University of Rochester	Romania	1
University of Rochester	Sweden	1
University of Rochester	Taiwan	2
University of Rochester	Turkey	2
University of Rochester	United Kingdom	9
Waste Isolation Pilot Plant	Austria	1
Waste Isolation Pilot Plant	Canada	8
Waste Isolation Pilot Plant	China, People's Republic Of	1
Waste Isolation Pilot Plant	Denmark	1
Waste Isolation Pilot Plant	France	2
Waste Isolation Pilot Plant	Germany(Unified)	3
Waste Isolation Pilot Plant	Italy	2
Waste Isolation Pilot Plant	Korea, South	1
Waste Isolation Pilot Plant	Malaysia	1
Waste Isolation Pilot Plant	Mexico	3
Waste Isolation Pilot Plant	New Zealand	1
Waste Isolation Pilot Plant	Russia	1
Waste Isolation Pilot Plant	Spain	1
Waste Isolation Pilot Plant	Switzerland	1
Waste Isolation Pilot Plant	Taiwan	1
Waste Isolation Pilot Plant	United Kingdom	1
West Hackberry, LA - SPRO	Canada	1
Western Area Power Administration	Albania	1
Western Area Power Administration	Australia	2
Western Area Power Administration	Canada	11
Western Area Power Administration	France	1
Western Area Power Administration	Germany(Unified)	2
Western Area Power Administration	Honduras	1
Western Area Power Administration	India	3
Western Area Power Administration	Mexico	28
Western Area Power Administration	Nepal	1
Western Area Power Administration	New Zealand	2
Western Area Power Administration	Norway	1
Western Area Power Administration	Sweden	2
Western Area Power Administration	United Kingdom	2
Yucca Mountain Project Office	Belgium	1
Yucca Mountain Project Office	Bolivia	1
Yucca Mountain Project Office	Canada	11
Yucca Mountain Project Office	China, People's Republic Of	7
Yucca Mountain Project Office	El Salvador	4
Yucca Mountain Project Office	France	4
Yucca Mountain Project Office	Germany(Unified)	2
Yucca Mountain Project Office	Greece	1
Yucca Mountain Project Office	Guatemala	2
Yucca Mountain Project Office	Honduras	1
Yucca Mountain Project Office	India	9
Yucca Mountain Project Office	Italy	1
Yucca Mountain Project Office	Japan	3
Yucca Mountain Project Office	Jordan	1
Yucca Mountain Project Office	Kenya	1
Yucca Mountain Project Office	Korea, South	3
Yucca Mountain Project Office	Mexico	46
Yucca Mountain Project Office	Peru	1
Yucca Mountain Project Office	Philippines	1
Yucca Mountain Project Office	Romania	2
Yucca Mountain Project Office	Serbia-Montenegro	1
Yucca Mountain Project Office	South Africa	1
Yucca Mountain Project Office	Thailand	1
Yucca Mountain Project Office	Turkey	1
Yucca Mountain Project Office	United Kingdom	11
Total DOE Foreign National Assignees		**19,059**

Order Code RL34595

CRS Report for Congress

Intelligence Reform at the Department of Energy: Policy Issues and Organizational Alternatives

July 28, 2008

Alfred Cumming
Specialist in Intelligence and National Security
Foreign Affairs, Defense, and Trade Division

Prepared for Members and Committees of Congress

Intelligence Reform at the Department of Energy: Policy Issues and Organizational Alternatives

Summary

After the repeated urging of the Department of Energy (DOE), Congress in 2006 agreed to temporarily consolidate separate counterintelligence (CI) offices at the Department of Energy and the National Security Administration (NNSA) into a single CI office under DOE control. DOE had complained that the dual office structure was ineffective. In permitting DOE to consolidate the two offices, Congress reversed its 1999 authorization to establish a separate NNSA CI office — a decision that at the time was prompted by congressional concerns over repeated departmental security and counterintelligence lapses.

At the same time, in 2006, DOE combined its separate Offices of Intelligence, and Counterintelligence into a new DOE office called the Office of Intelligence and Counterintelligence. The Department reasoned that combining the disciplines of counterintelligence and foreign intelligence under one integrated office would foster synergistic cooperation that would lead to a more strategic and ultimately more effective counterintelligence program.

This report analyzes both consolidations — the first authorized by Congress at DOE's request; the second initiated by DOE — and examines the impact of each on the effectiveness of the Department's CI program. A major oversight issue for Congress is whether either, or both, organizational changes will strengthen the Department's CI program as intended. Some observers are concerned that the two consolidations may have undercut CI capabilities.

Congress could maintain the status quo or choose from several alternative organizational approaches, some of which continue to be discussed despite the most recent organizational changes to the Department's CI program. Such alternatives range from maintaining the consolidated DOE/NNSA CI office but reversing DOE's decision to combine its formerly independent offices of foreign intelligence and counterintelligence, to eliminating both consolidations.

Congress also could exercise several oversight options, ranging from conducting classified CI briefings to commissioning a formal assessment of DOE's current CI reorganization.

This report will be updated as warranted.

Contents

Intelligence Reform at the Department of Energy: Policy Issues and Organizational Alternatives

Introduction

DOE Counterintelligence Critiques

Since its establishment in 1977, DOE has been repeatedly criticized for its security and counterintelligence efforts — viewed as being so seriously deficient that some observers believe DOE, through its actions, has "invited attack by foreign intelligence services."[1] The General Accounting Office,[2] the President's Foreign Intelligence Advisory Board, and the Intelligence Community, as well as DOE's own inspector general and security experts, collectively have issued numerous classified and public reports — according to some estimates, more than 100 — in the last 30 years that have highlighted a litany of DOE security and counterintelligence vulnerabilities. Because of these vulnerabilities, many believe that sensitive nuclear weapons information has "certainly" been lost to espionage. In countless other instances such information has been left vulnerable to theft and duplication.[3] Although the damage to national security resulting from such lapses has been difficult to calculate, DOE has been warned on many occasions that its "lackadaisical oversight" could lead to an increase in the nuclear threat to the United States.[4]

According to some analysts, given DOE's unwieldy bureaucratic structure, security lapses should not be viewed with surprise. DOE was established in 1977 by combining 40 diverse government organizations. The intention was to harness the Nation's research laboratories as part of a coordinated government effort to confront an energy crisis brought on in part by creation of OPEC.[5] Each agency, however, came with its own bureaucratic structure and culture, and many had different if not conflicting missions.

---

[1] See President's Foreign Intelligence Advisory Board, Science At Its Best/Security At Its Worst, June, 1999, pp. 2-3. The report, one of the most comprehensive of its kind, is often referred to as "The Rudman Report," in recognition of former U.S. Senator Warren B. Rudman, who served as Chairman of the President's Foreign Intelligence Advisory Board at the time the report was issued.

[2] The U.S. General Accounting Office is now known as the U.S. Government Accountability Office.

[3] See President's Foreign Intelligence Advisory Board, Science At Its Best/Security At Its Worst, June, 1999, p. 13.

[4] Ibid, p. II.

[5] The Organization of Petroleum Exporting Countries.

The agencies also differed in the importance they attached to security and CI. Some, such as the Energy Research and Development Administration, home to the Nation's highly sensitive nuclear weapons program, viewed such matters as being relatively more important. Others, such as the as the Interior Department's Power Marketing Administrations, attached a low priority to such matters. These sometimes starkly diverging views, although having moderated over time, arguably contribute to the cross-currents and conflicting pressures that have bedeviled DOE's security program and contributed to its lapses from the outset.

These varying views in turn may stem from certain built-in and enduring tensions which to a large degree are inherent in DOE's four principal missions. Three of those missions — fundamental science, energy resources, and environmental quality — thrive, indeed depend on open scientific inquiry. It is DOE's fourth mission, national security, that demands that security be the backdrop for scientific inquiry.[6] The result is an ever-present potential for conflict and an enduring challenge to strike the right balance between open collaboration and partnership, and security. So serious have been the ramifications of this challenge, that one study has concluded DOE has never fully recovered from some of the internal contradictions growing out of its own complicated creation.[7]

Critics Blame Weak Counterintelligence (CI) on Several Factors

Although many critics blame DOE's security problems generally on the tension within DOE between open scientific inquiry and security, they tend to focus on what they characterize as, *inter alia*, three specific issues: a high turn-over of inexperienced top leadership, bloated and dysfunctional management, and an agency culture that views the discipline of counterintelligence with disdain.

High leadership turn-over has been an enduring problem, according to Department critics. They point to the eleven secretaries who have led the department over an almost 30-year period. Although some secretaries have pushed aggressive security reforms, they often have left office before having fully implemented their proposals. Following their departures, the proposed reforms may be discarded or forgotten. Another cited problem has been a lack of experience in national security among some of those who have served as Secretary. Although DOE spends almost a third of its budget — roughly 30 percent — on nuclear related functions, many of its top leadership have lacked prior experience in such matters. As a result, security and CI problems may often have been seen as lesser priorities, and decisions on such matters left to lower-ranking officials who often have lacked either the incentive or authority to take quick, decisive action.[8]

---

[6] DOE's national security program also depends on open scientific inquiry and international collaboration, but in a secure and classified environment.

[7] President's Foreign Intelligence Advisory Board, Science At Its Best/Security At Its Worst, June, 1999, p. 8.

[8] Ibid, p. 5.

A second factor cited, related to DOE's security record is the Department's management structure which has been characterized by critics as bloated and dysfunctional. Multiple bureaucratic layers reportedly have so diffused authority and left accountability so erratic that "it [accountability] is now almost impossible to find."[9] Consequently, security and CI shortcomings appear to have gone unaddressed.

Finally, critics blame DOE's culture for contributing to an environment in which legitimate CI concerns are viewed with ambivalence, at best, and open hostility, at worse. The environment, it is suggested, is in large measure a natural and somewhat ironic outgrowth of brilliance from DOE scientists, some of whom "bridle under the restraints and regulations imposed by administrators and bureaucrats who do not entirely comprehend the precise nature of the operation being managed."[10] Thus, to some extent the very brilliance of its employees is cited as a significant contributing factor to a bureaucratic culture which they say is thoroughly saturated with cynicism and disregard for authority, and cavalier in its attitude toward security.[11]

Fears That China Stole Nuclear Secrets Sparks CI Changes 1998

DOE's CI program received a particular serious jolt in 1998, when intelligence evidence surfaced that indicated the People's Republic of China (PRC) had successfully stolen nuclear weapons secrets from the Department's weapons complex. This information led the Clinton Administration to conclude that the Department's CI program was in serious trouble and that a program overhaul could not be put off.

In February 1998, President Clinton issued a decision directive (PDD-61) instructing DOE to implement 13 reforms, the balance of which was geared to strengthening the Department's CI program. Among the most significant of the reforms was one that required DOE to establish its first-ever independent counterintelligence office — known formally as the Office of Counterintelligence (OCI). The mission of the new office was to develop and implement a coherent and comprehensive CI policy. A senior Federal Bureau of Investigation (FBI) executive, with access to the Energy Secretary, was put in charge.

The President's directive contained several additional initiatives. One authorized the OCI director to oversee and fund all DOE's CI functions, including all direct CI operations and all of DOE's laboratory-based CI field offices.[12] A

---

[9] Ibid, p. 4.

[10] Ibid, p. 11.

[11] Ibid, p. 6.

[12] According to DOE, the Department currently operates 19 CI field offices, which are located at its laboratories, science centers, plants, and site offices throughout the complex. CI Field Offices are headed by Senior Counterintelligence Officers, seven of whom are senior federal officers, with the balance being laboratory contract workers with extensive CI experience. The mission of a CI Field Office is to develop and implement a CI program.

(continued...)

second initiative required that DOE laboratories be contractually obligated to meet certain CI goals, objectives, and performance standards. And lastly, senior laboratory CI personnel were given direct access to laboratory directors.

Under a 1999 follow-on implementation plan, the OCI director's authority was expanded to include control over all CI programming, funding, and personnel matters at DOE field offices.

PDD-61 represented an effort to address long-standing weaknesses in DOE's CI program. DOE's CI program historically had never had a bureaucratic home of its own. Instead, the program, invariably characterized as a "junior partner," was a component of a larger office – in the 1980s, the Office of Security, which was tasked with physically protecting DOE facilities, and in the 1990s, the Office of Intelligence, whose principal mission was to assess foreign weapons of mass destruction programs. In each instance, the offices' principal respective missions did not include the development of an aggressive, unified, and comprehensive CI program aimed at preventing espionage. And the development of such a program is generally considered not to have begun until President Clinton issued PDD-61.

PDD-61 addressed other perceived weaknesses as well. Among them: insufficient CI funding; inadequate Headquarters control and authority over its CI field offices; uneven and irregular access by the Department's CI officials to senior-level DOE management; inadequately trained DOE CI employees; and a strained relationship with the FBI, the agency DOE relied on for much of its counterintelligence investigative expertise and resources.[13]

The Turning Point

Concerns about DOE's CI program came to a boil in 1999, a year in which Congress became more fully aware of DOE's espionage vulnerabilities.[14] In March

---

[12] (...continued)
DOE also operates a cyber operational analysis center (OAC), which is managed by a senior federal CI officer.

[13] For a more detailed examination of the FBI's counterintelligence role at DOE, see Appendix 1.

[14] Media reports of a recent allegation of espionage with a DOE connection involved PRC spy Katrina M. Leung, who the FBI reportedly said was a 20-year Bureau informant they now suspect was a "double agent" who provided classified material to the PRC. Leung allegedly had affairs with two former FBI agents, William Cleveland Jr., who, until he resigned his post on April 10, 2003, was Director of Security, at DOE's Lawrence Livermore National Laboratory, and James Smith. Leung received probation after pleading guilty to a tax charge and lying. Smith pleaded guilty to a felony false statement charge in 2004 and was sentenced to probation and three months home confinement. Cleveland was never charged with a crime. See Josh Gerstein, "Court Hears Arguments Over FBI Agent Accused of Exposing Probe," *New York Sun*, March 8, 2006. FBI officials reportedly said at the time that every PRC counterintelligence case investigated by the Bureau since 1991
(continued...)

of that year, allegations surfaced that a scientist employed by the Los Alamos National Security Laboratory had failed to notify DOE officials of his contacts officials of the People's Republic of China (PRC). It also was alleged that the scientist, a Taiwanese-born American named Wen Ho Lee, had failed to properly safeguard classified material and had refused to cooperate with authorities with regard to certain security matters. Lee was fired from his research position at Los Alamos National Laboratory after allegedly failing a polygraph examination. He later pleaded guilty to one felony count of unlawful retention of national defense information.[15]

In May 1999, a bipartisan House Select Commission[16] charged that the PRC had stolen design information on the United States' most advanced thermonuclear weapons and was using the information to speed the building of its next generation of thermonuclear weapons. The Commission concluded that the PRC had been penetrating U.S. national weapons laboratories for years, and continued to do so.[17]

In June 1999, the President's Foreign Intelligence Advisory Board (PFIAB) issued an extraordinarily harsh assessment of DOE's security practices. The Board criticized DOE for the "worst" security record on secrecy that members said they had ever encountered.[18] It also reported that its examination had revealed a department in denial over its security and counterintelligence vulnerabilities and failures, and blamed DOE's decades-long record of security failures on poor organization and a failure of accountability. The Board concluded that with regard to security matters, DOE was dysfunctional and incapable of reform.[19]

Despite its harsh criticism, the PFIAB dismissed assertions that DOE had suffered wholesale losses of nuclear weapons technology as a result of espionage. The Board, concurred, however, with an earlier U.S. Intelligence Community assessment that had concluded the PRC had stolen classified U.S. nuclear weapons

---

[14] (...continued)
may have been compromised by Leung, including that involving Wen Ho Lee. See Susan Schmidt and Dan Eggen "FBI Assesses Potential Damage From Spy Scandal," *Washington Post*, April 13, 2003, p. A04.

[15] See James Sterngold, "Nuclear Scientist Set Free After Plea in Secrets Case; Judge Attacks U.S. Conduct," *New York Times*, September 14, 2000, p. A-1.

[16] The Commission was known formally as the Select Commission on U.S. National Security and Military/Commercial Concerns With the People's Republic of China and was chaired by then Rep. Christopher Cox.

[17] See the Select Commission on U.S. National Security Military/Commercial Concerns With the People's Republic of China, *Cox Commission*, H.Rept. 105-851, May 25, 1999, Overview, p. ii.

[18] See President's Foreign Intelligence Advisory Board, Science At Its Best/Security At Its Worst, June, 1999, p. 1.

[19] Ibid. pp. II-III.

information that probably enabled it to accelerate its development of nuclear weapons.[20]

To fix DOE's security problems, the PFIAB recommended that policymakers consider two options. The first option called for the creation of a semi-autonomous agency within DOE that would be strictly segregated from the rest of the department, be more mission focused and bureaucratically streamlined, and that would be devoted principally to nuclear weapons and national security matters. The Board cited the National Security Agency and Defense Advanced Research Projects Agency, both elements of the Defense Department, as models of this approach.

A second option called for the creation of a new agency that would be entirely independent of DOE and would be headed by an administrator who would report directly to the President. The National Aeronautics and Space Administration and the National Science Foundation were cited as models of this approach.

Congress Adopts PFIAB Recommendation

Over the opposition of the executive branch, which argued that PDD-61 offered the best approach to resolving DOE's security problems by mandating the establishment of a single, unified Office of Counterintelligence — Congress approved the PFIAB's first option and created a semi-autonomous agency within DOE. Designated the National Nuclear Security Administration (NNSA),[21] NNSA was placed in charge of all DOE national security-related nuclear programs.[22]

In establishing the new agency, Congress also created two separate counterintelligence offices — placing the first one at NNSA and the second at DOE, thus essentially codifying the Office of Counterintelligence initially established under PDD-61. DOE's office was made responsible for developing overall CI policy for both DOE and NNSA, but implementing that policy only at non-weapons facilities. NNSA's CI office, designated the Office of Defense Nuclear Counterintelligence (ODNCI), was given responsibility for implementing OCI-developed policy at NNSA's facilities, principally at the DOE weapons laboratories. The NNSA CI office was to focus on protecting classified nuclear and related defense technology at NNSA facilities, while DOE's CI office was to concentrate on safeguarding all other technology and DOE sites. The two offices were to share analytic and

---

[20] Ibid. p.4.

[21] NNSA facilities include the national laboratories (Los Alamos National Laboratory, Los Alamos, NM; Lawrence Livermore National Laboratory, Livermore, CA; and Sandia National Laboratories, Albuquerque, NM and Livermore, CA); NNSA's CI programs are located principally at these national laboratories, which also are referred to as DOE's "weapons laboratories." NNSA facilities also include the nuclear weapons production facilities (the Plantex Plant, Amarillo, TX; Kansas City Plant, Kansas City, MO; the Y-12 Plant, Oak Ridge, TN; the tritium operations facilities at the Savannah River Site, Aiken, SC; and the Nevada Test Site, NV); and a service center at Albuquerque, NM. The U.S. Navy reactor facilities also fall under NNSA.

[22] See S. 1059; conference report, H.Rept. 106-301; and P.L. 106-65, signed into law on October 5, 1999.

investigative resources, leading some observers to characterize the arrangement as a "partially bifurcated" CI program.

Is a "Bifurcated" CI Structure Effective?

Critics of the new structure questioned its effectiveness and in 2002, the Commission on Science and Security,[23] issued a report criticizing the bifurcated program. The Commission's report recommended that DOE reestablish a single, unified program under the Department's control that would be responsible for counterintelligence across the DOE complex, including NNSA. The Commission's report stated:

> Counterintelligence must be an enterprise-wide function, responsible for counterintelligence issues anywhere within the DOE complex. Furthermore, counterintelligence investigations, analysis, and all other counterintelligence information must be developed within a unified organization and provided to the Secretary and other senior officials without bureaucratic delays. This vital function necessitates one organization with one chief of counterintelligence reporting to the office of the Secretary.[24]

In urging the adoption of a unified CI program, the Commission said foreign adversaries do not limit their espionage efforts to NNSA but search out attractive targets across the DOE/NNSA complex. Moreover, they stated that visiting foreign scientists, many from countries thought to be interested in conducting espionage at DOE facilities, often travel to both DOE and NNSA sites.

A second study, issued in 2003 by the Office of the National Counterintelligence Executive (NCIX),[25] similarly concluded that the bifurcated structure "not only served to further complicate the formidable challenge of managing CI at DOE, but also endangered the goals and implementation of an effective CI program."[26]

---

[23] The Commission on Science and Security was established in October 2000 at the request of then-Energy Secretary Bill Richardson to "...assess the new challenges facing the Department of Energy in operating premier scientific institutions in the twenty-first century in a manner that fosters scientific excellence and promotes the missions of the Department, while protecting and enhancing national security." See Commission on Science and Security, Science and Security in the 21st Century, A Report to the Secretary of Energy on the Department of Energy Laboratories, April 2002, p. 82. By the time the Commission completed its report in 2002, former U.S. Sen. Secretary Spencer Abraham had replaced Bill Richardson as DOE Secretary.

[24] Commission on Science and Security, Science and Security in the 21st Century, A report to the Secretary of Energy on the Department of Energy Laboratories, April 2002, p. 26.

[25] The Office of the National Counterintelligence Executive is part of the Office of Director of National Intelligence. One of its principal missions is to develop, coordinate, and produce an annual national CI strategy for the U.S. Government.

[26] See National Counterintelligence Executive, *An Assessment of the Effectiveness of the Division of the CI Programs at the Department of Energy and the National Nuclear Security Administration*, 2003. p. 1.

The NCIX report also stated that, "In light of the history of CI investigations that foundered because of mis-communications within well-established agencies, the two-office arrangement has raised the odds of missteps and problems."[27]

NCIX blamed the dual-office structure for numerous day-to-day problems, including duplicative and, at times, contradictory messages to field sites; mis-routed sensitive CI information related to investigations; uncoordinated communications to the FBI and the Intelligence Community; and dual, sometimes, inconsistent, program tasking.[28]

According to one law enforcement officer interviewed by NCIX during the preparation of its report, the two-office configuration "might some day lead the department to miss a serious CI breach or prevent the conduct of an effective investigation."[29] NCIX recommended that the two CI offices be consolidated within DOE under one senior counterintelligence officer who would be responsible for a Department-wide CI program and report directly to the Energy Secretary.[30]

The Directors of Central Intelligence and the FBI endorsed the NCIX findings in separate letters to the Chairman and Vice Chairman of the Senate Select Committee on Intelligence.[31]

In 2003, DOE Secretary Spencer Abraham publicly joined the debate, arguing that partially bifurcated structure was "not optimal." DOE had continued to complain that the structure impeded the smoother functioning of the Department's security operations. The Secretary recommended that the two offices be combined and placed under the control and authority of DOE.[32]

Debate Over Twin Office Effectiveness Continued

Despite the criticism, proponents of the new CI structure touted its effectiveness, arguing that the NNSA office was focusing the kind of sustained attention on CI at the laboratories that Congress had been demanding. They argued that NNSA's separate, dedicated CI office was vital if CI at NNSA's weapons laboratories was to receive the sustained attention Congress expected. They also said

---

[27] Ibid. p. 2

[28] Ibid. p. 10.

[29] Ibid. p. 13.

[30] Ibid. p. 3

[31] See letters from Director of Central Intelligence George Tenet, June 9, 2003, and from FBI Director Robert Mueller, July 11, 2003. Both letters were introduced into the record during a July 13, 2004 hearing on DOE counterintelligence consolidation conducted by the House Energy and Commerce Subcommittee on Energy and Air Quality.

[32] For a more complete discussion of DOE's position on the issue of CI bifurcation, see testimony presented by Linton Brooks, Administrator, National Nuclear Security Administration, before the House Energy and Commerce Committee, Energy and Air Quality Subcommittee, July 13, 2004.

that the bifurcated structure had proven successful in other DOE programs that shared jurisdiction. They instead blamed any significant problems on ineffective and non-cooperating program managers, rather than on the structure itself.

As each of the offices began to take on their own identities, Members of Congress also appeared to develop diverse views of the effectiveness of the two office structure. Rather than recombine the two offices under DOE control, as Secretary Abraham had recommended, the Senate Armed Services Committee approved the establishment of a single CI office, but placed it under NNSA control. The House Armed Services Committee objected, and the Senate's proposal died in conference. But, the Conferees did agree to urge the two offices to improve cooperation, noting in their report:

> ....that the NNSA was originally set up as a semi-autonomous agency, in large part, to ensure that there would be adequate focus and priority placed on counterintelligence activities. The conferees urge the counterintelligence offices at DOE and NNSA to work together to ensure security of both DOE and NNSA programs and facilities."[33]

Congress Changes Course; Eliminates DOE/NNSA Bifurcation and Authorizes Program Consolidation

In 2007, Congress reversed course, albeit reluctantly, and consolidated the two CI offices into a single office within DOE.[34] In agreeing to DOE's recommendation, however, Congress said it remained un-persuaded the Department had "fully and faithfully" implemented the counterintelligence structure authorized in 1999, and it stated that any of the perceived problems thought to stem from having two CI offices could have been resolved by applying "greater management resourcefulness."[35]

Congress said it remained skeptical that DOE could implement a strong security program. Alluding to the Wen Ho Lee case, the Conference warned that re-consolidation, together with DOE's internal decision to combine its own Offices of Intelligence and Counterintelligence under a new Office of Intelligence and Counterintelligence, would leave DOE's counterintelligence functions "organized as

---

[33] The 108th Congress voted to retain the bifurcated CI structure. See Conf. Rept. 108-767, p. 897, accompanying H.R. 4200, the FY2005 defense authorization bill.

[34] P.L. 109-364, Sec. 3117. The legislation approved by Congress calls for the disestablishment of NNSA and the transfer of its Office of Defense Nuclear Counterintelligence to DOE's Office of Counterintelligence, but under a sunset provision, would reestablish NNSA's CI office in 2010. As result of DOE's internal consolidation of its intelligence and counterintelligence offices in March 2006, the Office of Counterintelligence no longer exists, per se. Counterintelligence is now over seen by the Directorate of Counterintelligence, which is a component of DOE's recently established Office of Intelligence and Counterintelligence.

[35] Conference Rept. 109-702 (2nd Sess.), p. 769, accompanying H.R. 5122, the FY2007 John Warner Defense Authorization Act, which became P.L. 109-364.

they were when the Department experienced significant counterintelligence problems."[36]

Congress adopted legislation that included some "safeguards." First, the legislation contained a "sunset" provision that effectively would reestablish NNSA's CI office in 2010. Second, the legislation established an Intelligence Executive Committee within DOE to develop and promulgate CI policies. The NNSA Administrator was designated a committee member. Third, the legislation established a new position — the Intelligence and Counterintelligence Liaison — within the staff of the NNSA Administrator to act as a liaison between NNSA and DOE's Office of Intelligence and Counterintelligence. Lastly, the legislation required that DOE detail in its annual congressional budget submission the level of funding requested for counterintelligence activities overall and the amount of such counterintelligence funding requested by NNSA.[37]

Proponents of DOE/NNSA Consolidation Say It Strengthens CI

Proponents of consolidating all counterintelligence programming within DOE argue that such a unified structure has provided a number of benefits.

One such benefit, according to proponents, is increased accountability. Rather than relying on two CI program managers with divided accountability, the Energy Secretary and the NNSA Administrator now can hold a single individual ultimately accountable for a single, unified Department-wide CI program.

Another benefit proponents cite — one that the Commission on Science and Security underscored in its reported in 2002 report — is that consolidation has provided DOE a unified bureaucratic structure through which the Department can more effectively centralize control over CI programming across the DOE complex. Under the previous partially bifurcated structure, responsibility for CI was shared between the two offices. DOE's Office of Counterintelligence developed CI policy, which NNSA's CI office then implemented at NNSA facilities. The arrangement was said to lead to disagreements between the two offices, and DOE's CI officials questioned whether its NNSA counterparts were exceeding their mission and developing their own CI policies. On this point, NNSA officials countered that DOE failed to develop comprehensive and effective policies, and they therefore were left with no choice but to develop their policies when necessary. Proponents and critics appear to agree that the bifurcated structure contributed to the development of divergent management philosophies, priorities, and interpretations and

---

[36] Ibid.

[37] P.L. 109-364, Sec. 323 states, "...In the budget justification materials submitted to Congress...the amounts requested for the Department for intelligence and the amounts requested for the Department for counterintelligence functions shall each be specified in appropriately classified individual, dedicated program elements. Within the amounts requested for counterintelligence functions, the amounts requested for the National Nuclear Security Administration shall be specified separately from the amounts requested for other elements of the Department."

implementation of DOE CI guidance, and resulted in inconsistent CI practices across the DOE/NNSA complex.[38]

A third benefit, one highlighted by NCIX in its 2003 report, is that consolidation has eliminated, or certainly reduced, the occurrence of certain day-to-day problems that stemmed from a two-office structure in which responsibilities sometimes overlap. These problems reportedly included duplicative and at times contradictory messages issued to field sites, mis-routed sensitive investigative CI information, and uncoordinated communications to the FBI and the Intelligence Community.

Finally, consolidation, it is argued, has provided the official in charge of DOE's CI program — the Secretary of Energy's Senior Intelligence Officer (SIO) — exclusive authority to develop and implement a more strategically-oriented DOE-wide CI policy. This is particularly important, it is suggested, given that NNSA's program was perceived as largely tactical, reactive, and ultimately geared to uncovering espionage after the fact. According to proponents, consolidation has resulted in the development of a more strategic, and therefore stronger CI program — one that focuses predominantly on using foreign intelligence to determine what DOE information and computer networks are most at risk of espionage. Equipped with this knowledge, CI officials, the argument goes, increasingly have been able to construct an aggressive CI program focused on preventing espionage before it occurs. "We want to harness foreign intelligence to support counterintelligence," said one CI official. "If we can understand the offense (the plans and intentions of foreign intelligence services), we can harness it."[39] Proponents point to the development of the "Common Operational Picture" tool as an example of the kind integrative initiatives that have been launched as a result of consolidation. This particular tool provides CI officials a method by which to represent the CI threat geo-spatially, permitting that CI analysis can be captured collaboratively and comprehensively across the DOE/NNSA complex.

In pointing to the benefits of the NNSA/DOE consolidation, however, proponents caution that a recent decision to transfer a substantial number of CI headquarters staff to another location within the Washington metropolitan area could have the effect of undercutting some of those benefits. The transfer, they argue, the result of limited classified space at Headquarters, could undermine efforts to improve program integration and ironically create another type of bifurcation.

Critics Cite Negative Impacts of DOE/NNSA CI Consolidation

Consolidation critics do not dispute that a unified office and single chain of command improves accountability, but they cite several reasons why DOE/NNSA consolidation has undercut the CI capabilities.

First, NNSA's CI office focused exclusively on counterintelligence. In contrast, DOE treats CI as a component of a larger integrated office — the Office of

---

[38] Interviews with DOE officials, September-October, 2007.

[39] Interview with senior DOE official, July 11, 2007.

Intelligence and Counterintelligence — that also includes a Foreign Intelligence Directorate (FI), which, among other tasks, assesses intelligence in order to identify those DOE technologies most likely to be the target of espionage.[40] As result of placing CI within a larger structure, according to critics, DOE is unable to match NNSA' s more focused treatment. On this point, consolidation proponents argue that DOE has always used all appropriate information and resources from the intelligence, security and law enforcement communities to address CI concerns.

Compounding what they view as a structural bias is DOE's decision to devote comparatively more time, attention, and resources to developing its foreign intelligence capabilities. This, critics suggest, has come at the expense of CI capabilities.

Critics describe an emerging programmatic imbalance between foreign intelligence (FI) and CI. They point to DOE's history, which is one in which CI often has been relegated to a secondary or supporting role, first to the DOE's physical security program in the 1980s and 90s, and now possibly to its FI program. These critics argue that it is this historic trend that prompted Congress to establish NNSA's CI office in the first place. It was not lost on Congress, according to one senior CI official, that DOE headquarters was "detached from the field reality" when it came to dealing with CI issues. DOE Headquarters officials concede they have decided to increase the focus on FI but that they are doing so as part of an overarching strategic effort, the goal of which is to more effectively harness FI to support of CI. They dispute that such support has come at the expense of counterintelligence.

Second, NNSA CI managers, some suggest, simply were more effective than their DOE counterparts have been under the consolidated arrangement. It is suggested that NNSA managers developed and implemented a number of laudable practices. Among them: frequent communication between NNSA headquarters and field personnel; regular laboratory visits by NNSA Headquarter CI officials; consensus building on CI tactics and strategy; effective follow-up; and relatively quick decision-making. Even in the one area some critics credit DOE's consolidated program for emphasizing — strategic CI — they fault DOE for what they argue has been its failure to take and resolve some of strategic issues that are integral to any successful strategic plan.

Third, NNSA's CI methods and techniques were generally more effective than those now being employed by DOE. Critics say the difference is one of emphasis. NNSA placed greater reliance on non-confrontational briefings and debriefings of laboratory employees, an approach that consolidation critics contend is more effective in ferreting out espionage. DOE, it is suggested, is taking a harder-edged, investigative approach. One critic, for example, compares DOE's approach to "dragnet tactics that assume folks are guilty until proven innocent."[41] NNSA, according to this critic, pursued investigations when necessary, but generally relied

---

[40] The Intelligence Directorate operates Field Intelligence Elements, which are located at some DOE laboratories and assess intelligence related to science and technology trends and foreign nuclear weapons systems.

[41] Interview with senior DOE official, December 13, 2007.

on less aggressive techniques, in the belief that such an approach would generate more useful information about possible espionage. "[NNSA's philosophy] relied on the workforce to help you," this observer suggested. On this point, consolidation proponents contend that DOE's CI program has always employed a multi-disciplined approach incorporating various CI tools such as investigations, analysis, cyber activities, and CI training and awareness. They also argue that both programs were mandated to follow the same CI procedures.

Despite these disagreements, critics and proponents appear to agree that a unified CI program under a single chain of command is preferable. Consolidation critics, however, suggest that the ultimate success of any CI program depends more on effective leadership than its does on any particular bureaucratic structure. In this regard, they state that DOE in the past has overseen a consolidated program and argue that program effectiveness was undermined by ineffective leadership. One consolidation critic conceded that the establishment of NNSA's CI office may have represented little more than an effort to "work around" what some viewed as DOE's historically weak CI management.[42]

Consolidation proponents counter that the DOE/NNSA consolidation has been in place only since the beginning of 2007, and that it is taking root in the aftermath of a prolonged period of organizational turmoil characterized in part by high management turnover.[43] As a result, they argue, efforts to build consensus, improve communication, and foster collaboration are still in their infancy. They also question the quality of some of the CI evaluation assessments conducted by NNSA CI office and say that such assessments are now being undertaken in accordance with DOE and IC CI standards.

DOE Implements Internal Consolidation, Combining Offices of Intelligence and Counterintelligence

In 2006, the same year Congress agreed to consolidate the DOE and NNSA counterintelligence offices, DOE decided to combine its Offices of Intelligence and Counterintelligence under a new Office of Intelligence and Counterintelligence. The mission of the new office is to provide the Secretary, his staff, and other DOE policymakers with timely, technical intelligence analyses on all aspects of foreign nuclear weapons, nuclear materials, and energy issues worldwide.[44] The office is led by the Department's Senior Intelligence Officer, who reports directly to the Secretary of Energy.

The Office of Intelligence and Counterintelligence is comprised of four directorates: intelligence, counterintelligence, management, and energy and

---

[42] Interview with senior DOE official, December 12, 2007.

[43] Consolidation proponents say that four directors have led DOE's CI program since 1998, one of whom served only one year.

[44] See [http://www.energy.gov/organization/staffoffices.htm]. Although this particular Internet site contains no apparent mention of the Office's CI mission, the Office does contain a CI Directorate.

environmental security. The Directorate of Intelligence is tasked with assessing the capabilities, intentions, and activities of foreign powers, organizations, and persons who may be targeting DOE for espionage purposes. The Counterintelligence Directorate is charged with protecting DOE's classified information from espionage. The Management Directorate houses support activities for the other two directorates, including human resource services, contract support, and facility planning. And the Energy and Environmental Security Directorate is charged with examining the impact of certain energy and environmental issues on U.S. national security.

Proponents of FI/CI Consolidation Say it Has Strengthened CI

Proponents of this consolidation say that by establishing intelligence and counterintelligences directorates in a single office, DOE has strengthened its CI program.

Specifically, proponents contend a more integrated FI/CI structure will make it easier for the Department's Senior Intelligence Officer to foster cooperation between the two disciplines and to develop and implement a CI program that is both more synergistic and strategic in approach. Previously, the two programs worked together, but on a more independent basis that consolidation proponents argued was detrimental to both. Under the new arrangement, they say, communication, cooperation, and collaboration between two disciplines already have improved. As result, officials have been able to more effectively harness foreign intelligence analysis and use it to fashion more strategically focused CI plans that concentrate on what DOE information and computer networks are most at risk of espionage. Specifically, proponents point to increases in CI and FI collection, the number of investigative cases opened, and in the pace of offensive operations against national security targets. Further, DOE officials say the consolidation program conforms with the intent of the FY2004 Intelligence Reform and Terrorism Prevention Act, a major goal of which was to encourage the Intelligence Community to adopt a more integrated corporate approach.

Proponents also say that FI/CI consolidation has helped to correct a prevailing mis-perception within the Intelligence Community that DOE had two Senior Intelligence Officers — one for intelligence and one for counterintelligence. Although the Department always has had a single SIO, the organizational confusion reportedly contributed to weakening the SIO's overall program authority which in turn undercut accountability and the operational cohesion between FI and CI. "...Can we do the mission if CI and FI are separate?" one official asked. "I'm convinced you cannot."[45]

Proponents further suggest that consolidation has enabled DOE to begin the process of establishing an "intelligence brand," thus simplifying the challenge of distinguishing DOE's intelligence products from those of other Intelligence Community agencies. Doing so, according to these proponents, will help to reverse a commonly held Intelligence Community view that DOE's FI program is a mere extension of the CIA, and that its CI program an extension of the FBI, since detailees

---

[45] Interview with senior DOE official, July 17, 2007.

from the CIA and FBI respectively historically headed the two DOE programs. The argument is that establishing a "branding" will enable DOE to more effectively highlight DOE's unique contributions to policymakers.

Lastly, proponents suggest, consolidation has enabled DOE, through its SIO, to begin formulating and implementing a training program that eventually will lead to the development of DOE cadres of senior intelligence and counterintelligence professionals, thus ending its historic reliance on CIA and FBI detailees.[46]

Critics of FI/CI Consolidation Argue It Has Undercut CI Capabilities and Authorities

Critics point to what they contend are at least three indicators that CI/FI consolidation has undercut counterintelligence capabilities and authorities.

First, critics insist that CI resources at some laboratories have been cut, and they blame the reductions in part on increased FI spending. They point to at least two FI initiatives — the Energy Attache Program[47] and the Collection Management Initiative[48] — and suggest that funding for both has been provided at the expense of the CI program.

They also point to CI budget constraints, citing several other factors. Among them: a continuing resolution that kept CI spending flat, despite DOE requests for increase[49]; the transition of some DOE laboratories from non-profit to a for-profit status, which has resulted in higher payroll and other costs; and a reported DOE Headquarters CI contingency fund, which has resulted in 10 percent of the overall CI budget being held in reserve to cover unexpected costs.[50]

DOE Headquarters officials deny that CI funding has been diverted to support FI. Rather, they say they have increased spending for CI, but that those increases have gone unrealized because DOE has operated under short-term continuing resolutions since 2006. But they appear to generally agree with consolidation critics who attribute at least some of the blame for budget constraints on the non-profit to for-profit transition that is underway at some laboratories and the CI contingency fund. They contend, however, that no laboratory CI office is doing with less but that "each

---

[46] Interview with senior DOE official, July 17, 2007.

[47] This initiative is designed to place overt DOE Intelligence Attaches in U.S. embassies where they will focus on energy security issues.

[48] The Collection Management Initiative involves the production and dissemination of increased quantities of Intelligence Information Reports, raw intelligence reports derived from DOE intelligence collected passively from DOE personnel by DOE CI personnel.

[49] Critics assert that any lingering impact of the Continuing Resolution is long over and, yet, no field CI office has received any budget relief. They further contend that DOE's overall level of CI effort is decreasing, including at the NNSA laboratories.

[50] DOE CI and FI budget data are classified, preventing a more detailed unclassified examination.

office has gotten little more than the year before."[51] Critics counter that CI offices at each of the six largest laboratories — Los Alamos, Lawrence Livermore, Argonne, Pacific Northwest, Oak Ridge, and Sandia — have absorbed 10 percent funding cuts over the last year, despite increases in the DOE Headquarters CI budget and despite the fact that the Department is no longer operating under a continuing resolution.[52]

Second, critics say the authorities of CI Deputy Director have been eroded since the previously existing independent CI office was eliminated and absorbed by the Office of Intelligence and Counterintelligence. Whereas the director of that independent office controlled CI spending and staff, the CI Deputy Director in the new Office of Intelligence and Counterintelligence does not and that control resides with the Deputy Director of Administration. And while the Deputy Director, like his independent office predecessor, continues to have access to the Energy Secretary — generally viewed as one of PDD-61's more significant provisions — his access to the Secretary appears to be at the pleasure of the Director of Intelligence and Counterintelligence, to whom the Deputy Director now reports.

Third, critics say they are concerned by suggestions made to senior DOE officials that PDD-61 is dated and should therefore be placed on "an inactive status." Critics contend that some of the directive's most important provisions have been ignored, allowing the document to be characterized as "dated." They cite as an example the elimination of independent Office of Counterintelligence, a principal provision originally contained in the directive. Critics believe certain provisions, however, remain in effect and should be preserved. One such provision requires that DOE's laboratory contracts contain certain CI program goals, objectives, and performance measures. Another requires senior CI officials at the laboratories to have direct access to laboratory directors.

Those advocating that PDD-61 should be placed on an "inactive status" say they embrace the CI vision embodied in the directive but insist that some of its key provisions have been superseded by changes in law.[53] One change is that the role of the FBI director in selecting a DOE CI chief has been eliminated. [See Appendix for a general discussion of the FBI's role in DOE CI.] Under current law, the Secretary of Energy has that authority. Another change is that there is no longer a requirement that the CI chief be a senior FBI executive, which PDD-61 required. Finally, in another change, the Secretary is expected to "coordinate" his selection with the Director of National Intelligence, a relatively new position which was created under the FY2004 Intelligence Reform and Terrorism Prevention Act, and which did not exist at the time PDD-61 was issued in 1998. Under PDD-61, the FBI Director recommended a selection to the Attorney General.

Despite these concerns, critics say they agree that communication between FI and CI officials could be improved. But, they question whether this goal could have

---

[51] Interview with senior DOE official, December 19, 2007.

[52] E-mail exchange with senior DOE official, February 25, 2008.

[53] Interview with senior DOE official, July 17, 2007.

been achieved through means other than a wholesale reorganization which they characterize as highly disruptive.

Concerns of some CI officials that FI/CI consolidation has weakened CI capabilities and authorities appear to run deep.[54] One senior CI official has reportedly resigned because of cuts to his laboratory's CI program. According to another CI official, budgets for CI programs at DOE's six largest laboratories were cut at the beginning of FY2008, despite a double-digit increase in the Department's overall CI budget.[55] These funds, according to this official, are being used to fund projects at DOE Headquarters. As a result of the cuts, this official said, CI analytic capability has been degraded.

Some CI officials argue that CI program managers increasingly are being asked to carry out FI assignments, the result of which, in some cases, is to reduce the time and resources devoted to CI. "We watched this (de-emphasis of CI) go into peaks and valleys...it is a huge mistake to demote CI to FI."[56] One laboratory CI official, concerned by what he perceived to be a diminution of CI, but also by the general level of disruption resulting from consolidation, complained that, "Until the (CI/FI) reorganization, I spent 10 percent of my time on Headquarters stuff. Now it's reversed." He said the CI/FI consolidation itself was "unraveling." "(DOE) Headquarters doesn't appreciate how deep the field concerns are," another said, referring the views of CI officials at DOE's weapons laboratories.[57]

These officials contend that communication between Headquarters and the laboratories — never very good — has been made worse by the consolidation. Finally some officials complain that although one of the principal objectives of consolidation was to foster a more strategic approach to CI, that certain strategic goals are not being met. They cite as examples DOE's inability to adequately address issues of personnel security clearances, and the CI implications of DOE interactions with foreign scientists, whether such interactions occur with visiting scientists in the Department's laboratories, or when DOE laboratory employees travel overseas.

Consolidation proponents acknowledge such criticisms, but suggest they underscore continuing communication problems between DOE Headquarters and CI field offices rather than an actual diminishment in CI operational capabilities.[58] They also suggest that there are "misperceptions about how DOE Headquarters is managing overall CI spending, but insist that the each of DOE's six largest

---

[54] This impression was derived from a series of interviews conducted with senior DOE officials in October of 2007.

[55] According this official, since the beginning of the fiscal year funding in the case of some laboratories has been restored, at least in part.

[56] Interview with senior DOE official, November 2, 2007.

[57] Interview with senior DOE official, October 17, 2007.

[58] E-mail from senior CI official, April 28, 2008.

laboratories has received "budget/spending" authority increases in FY2008.[59] Finally, they concede that some observers could conclude that some CI funding is being used to support FI efforts — critics have cited CI spending in support of the new collection management initiative — but argue that such spending ultimately has served CI interests.[60]

Finally they characterize the consolidated business model DOE Headquareters has adopted as sound and emphasize that consolidation is a work in progress beset by normal organizational growing pains.[61]

Possible Organizational Alternatives

Congress may deem the current approach to be the appropriate one, which would have the effect of reestablishing NNSA's CI office in 2010 and retaining DOE's FI/CI program consolidation. If organizational changes are sought, policymakers might consider several questions. First, should the 2010 sunset provision currently in law be retained and NNSA's CI office be reestablished in 2010? Second, should DOE's FI/CI consolidated program be retained, or should Congress direct DOE to reestablish independent FI and CI offices within DOE? Within the context of these two overarching questions, the range of possible options include (1) eliminate the 2010 sunset provision contained in P.L. 109-364 and *not* reestablish NNSA's CI office in 2010; retain DOE's FI/CI consolidated program; (2) maintain the 2010 sunset provision and reestablish NNSA's CI office, but as an office *independent* of DOE, dropping the previously existing bifurcated CI structure; retain DOE's FI/CI consolidated program; (3) eliminate both the 2010 sunset provision and DOE's FI/CI consolidated program, reestablishing independent FI and CI offices within DOE; (4) maintain the 2010 sunset provision and reestablish NNSA's CI office, but *consolidate within that office* DOE's CI directorate; retain DOE's FI/CI consolidated program; (5) maintain the 2010 sunset provision and reestablish NNSA's CI on a bifurcated basis under which NNSA and DOE would share certain CI resources; eliminate DOE's FI/CI consolidated program and reestablish independent FI and CI offices within DOE; and (6) place the FBI in charge of DOE CI.

Alternative One: Eliminate the 2010 Sunset; Retain DOE's FI/CI Consolidation

This approach would eliminate the sunset provision contained in P.L. 109-364 and *not* reestablish NNSA's CI office in 2010 while retaining DOE's FI/CI consolidated program. Proponents could argue that in doing so, the gains resulting from the DOE/NNSA consolidation — improved accountability and enhanced CI capabilities — could be preserved and expanded. With regard to DOE's consolidated

---

[59] Ibid.

[60] Ibid.

[61] Ibid.

FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Opponents could argue that retaining the sunset provision and reestablishing NNSA's CI program would bring needed attention and focus to CI in DOE's weapons laboratories. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Alternative Two: Maintain the 2010 Sunset But Establish an Independent NNSA CI Office; Retain DOE's FI/CI Consolidation

A second alternative would be to maintain the sunset provision and to reestablish NNSA's CI program in 2010, but as an independent entity unencumbered by the previously existing bifurcated structure; DOE's FI/CI consolidated program would be retained. Under the previously existing structure, NNSA's CI office was restricted to implementing DOE CI policy, and it shared certain analytic and investigative resources with its DOE counterpart.

Proponents could argue that an independent NNSA CI office could be more effective than its predecessor, since, under this alternative, the office would have the responsibility for both developing and implementing CI policy at all NNSA facilities. They could assert that this approach could eliminate the tensions and bureaucratic inefficiencies that resulted from the previous twin office structure. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Opponents could argue that re-establishing NNSA's CI office could disrupt the continuity and progress that have resulted under the current consolidated arrangement. They also could assert that establishing an independent CI office at NNSA could require additional funding, since the office would no longer be sharing certain resources with its DOE counterpart. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Alternative Three: Eliminate Both the 2010 Sunset and DOE's FI/CI Consolidation

A third alternative would be to eliminate the sunset provision contained in P.L. 109-364 and to *not* reestablish NNSA's CI office in 2010. DOE's FI/CI consolidated program also would be eliminated under this alternative and an independent CI office with budget control reestablished. Proponents could argue that eliminating the sunset provision would eliminate redundancies and additional costs that result from a dual or bifurcated CI program management structure. Eliminating DOE's consolidated FI/CI program, it could be argued, would address the concerns expressed by some that CI interests have been subordinated to FI priorities.

Alternative Four: Maintain the 2010 Sunset Provision But Consolidate All CI Within NNSA; Retain DOE's Consolidated FI/CI Program

A fourth alternative would be to maintain the sunset provision and reestablish NNSA's CI office in 2010, but shift control over all CI program functions, including DOE's, to the new NNSA office; DOE's FI/CI consolidated program would be retained.

Proponents could argue that the reestablishment of an NNSA office under which all CI, including DOE's, would improve program effectiveness because of NNSA's record focusing more attention on CI. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Opponents could contend that such an approach could disrupt DOE's continuing efforts to construct a strategic CI program within the Department and jeopardize the gains that have been achieved. They also could argue that NNSA's previously existing CI office was overly tactical in its approach to CI and failed to place sufficient emphasis on strategic issues. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Alternative Five: Maintain 2010 Sunset; Eliminate DOE's Consolidated FI/CI Program

This approach would eliminate both organizational consolidations — the NNSA/DOE CI consolidation as well as DOE's FI/CI consolidation. Proponents could argue that such an approach would strengthen CI authorities and capabilities by restoring NNSA's CI office and an independent CI office within DOE.

Opponents could argue that reversing the two consolidations could undermine the benefits derived from having a more CI integrated program interacts more closely with the FI discipline.

Alternative Six: Place FBI in Charge of DOE CI

Under this approach, Congress could eliminate DOE's CI program altogether and place it under the FBI's authority. Although the FBI currently has special agents co-located at certain laboratories, under this alternative, these agents would take on more assertive leadership roles.

An advantage of such an alternative is that the FBI is the government's premiere CI organization, and therefore is arguably uniquely suited by training and experience to undertake this task.

A disadvantage could be that an FBI-controlled CI program could have a chilling effect on the possible cooperation of DOE employees, particularly scientists

and engineers, who historically have chaffed at FBI's involvement in DOE's CI program.

Maintain the Legislative Status Quo

Under this approach, the NNSA/DOE CI consolidation would be reversed in 2010 and NNSA's CI office reestablished; DOE's FI/CI consolidated program would be retained.

Proponents of the status quo could contend that the NNSA/DOE consolidation has failed to improve accountability and overall CI program effectiveness. With regard to DOE's consolidated FI/CI program, they could argue that gains made as a result of consolidation could be preserved and expanded by retaining the current structure.

Opponents could argue that NNSA's CI program was effective and should be reestablished. With regard to DOE's combined FI/CI program, they could argue that consolidation has undermined CI authorities and capabilities and had the effect of relegating CI to a "second-class" status within the Department.

Possible Oversight Alternatives

The Congress also could consider adopting one or more of several oversight alternatives. The range of alternatives includes (1) instituting classified CI briefings; (2) commissioning a formal assessment of the benefits derived from DOE's FI/CI consolidation; (3) ensuring DOE compliance with current law; and (4) codifying portions of PDD-61.

Alternative One: Classified Congressional CI Briefings

Congress could require that DOE brief the appropriate congressional committee or committees on the types of CI methods being used, especially on the Department's most significant pending CI cases.

An advantage of such an approach would be that it could provide Congress with significant new insight into DOE's overall CI efforts. Such briefings could also lead to a better understanding of the strategic interests of certain foreign powers and could provide insights into how effectively DOE is interacting and cooperating with the Intelligence Community at large.

A disadvantage of this alternative would be that such briefings could be considerably time-consuming; the number of such cases can be numerous, detailed, and complicated. Such cases also are invariably quite sensitive. DOE might try to restrict such briefings to committee leadership. As a result, committee leadership could find themselves assuming a significant oversight responsibility.

Alternative Two: Commission a Formal Assessment of FI/CI Consolidation

A second approach would be for Congress to commission an assessment of any benefits that have been derived from the DOE FI/CI consolidation. Such an assessment could enable Congress to better evaluate whether the consolidation has indeed improved communication between the two disciplines, as DOE has suggested. As part of such an assessment, the Department's Senior Intelligence Officer could be requested to demonstrate with concrete examples how the Department's FI/CI consolidated program has led to certain program synergies which could not have otherwise been achieved through greater management resourcefulness.

Other than the cost that may be associated with conducting such an assessment, there is no apparent disadvantage to such approach.

Alternative Three: Review DOE Compliance With the Law

Another approach Congress could pursue is to ensure that DOE complied with the law when it consolidated the Office of Intelligence and Counterintelligence under the new Office of Intelligence and Counterintelligence. Some have questioned whether the consolidation is consistent with current law, suggesting that consolidation amounted to a "transfer of function" from the Office of Counterintelligence or the Office of Intelligence to a new layer of bureaucracy within the Office of Intelligence and Counterintelligence. [62]

Alternative Four: Codify Relevant Parts of PDD-61

Under this approach, Congress could codify certain PDD-61 provisions. Two such provisions could be viewed as being particularly relevant. The first requires that DOE's laboratory contracts contain specific CI goals, objectives, and performance standards. The second provision stipulates that senior laboratory CI personnel be granted direct access to laboratory directors. Codifying these provisions would ensure that they are legally binding and not subject to termination by administration fiat.

A possible disadvantage of such a approach is that it could limit certain executive branch flexibility.

---

[62] For a more detailed treatment of this issue, see S.Rept. 109-259, which accompanied S. 3237, the FY2007 Intelligence Authorization Act, pp. 44-45. The Senate Select Committee asserted that DOE's "consolidation effort is arguably inconsistent with current law." The Committee said that such an inconsistency would exist if the consolidation amounted to a "transfer of function" from the Office of Counterintelligence or the Office of Intelligence to a new layer of bureaucracy within the Office of Intelligence and Counterintelligence.

Appendix

The Historical Role of the FBI[63] in the Development of the DOE CI Program. The 1998 PDD-61 formalized what until then had been a more informal FBI role in supporting DOE's CI Program. The directive established an independent Office of Counterintelligence and directed that the FBI director select and place in charge of the office a senior FBI representative.

A more recent example of the FBI's formal role is the joint FBI-DOE "Agents-in-the Labs" (AIL) Program. The AIL Program is designed to support the FBI Counterintelligence Division's strategic priorities, which include:

1. Preventing or neutralizing the foreign acquisition of weapons of mass destruction (WMD) technology or equipment;

2. Preventing the penetration of the Intelligence Community, U.S. Government, or contractors;

3. Preventing the compromise of U.S. critical national assets; and

4. Conducting aggressive CI operations against most significant threat nations.[64]

Under this program, the FBI has 16 Special Agents at 12 DOE locations working with DOE CI professionals to execute the CI mission.[65]

Despite its expanded role, the FBI has more recently lost some of its authority over the program. Congress eliminated the FBI director's authority to select a director for DOE's CI program, and the individual serving in that role is no longer required to be a senior FBI executive. Under current law, the Secretary of Energy now exercises the selection authority. (See Table 1 below).

Whether the congressional action eliminating the FBI's role in the selection process will result in the diminishment of the FBI's role in DOE's CI program continues to be the debated. Whether FBI assumes a diminished role turns in part on whether DOE develops the capability to recruit, train, and retain its own CI

---

[63] The FBI has played and continues to play an important role in the CI Program because it is lead agency for counterintelligence within the United States, where all DOE labs are located. It should be noted, however, that even within the discipline of counterintelligence there are differing approaches. Arguably, the FBI's approach relies heavily, although not exclusively, on CI investigations and operations to prevent espionage. While foreign intelligence agencies recognize the importance of investigations, generally, their CI focus is on understanding how the adversary operates to collect intelligence and proactively engaging in tactics to prevent the adversary's techniques from being successful. Military CI organizations, generally, tend to view CI through the prism of force protection and use a variety of CI tools to reach that end. CRS is unaware of any empirical studies which have assessed how these approaches have performed relative to one another.

[64] Interview with FBI officials, November 6, 2007.

[65] Ibid.

professionals and thus reduce its historical reliance on the FBI. If it is unable to do so, FBI's potentially diminishing role could be viewed in a less positive light.

Table 1. Statutory Role of the FBI in the DOE CI Program

Authority	Role of the FBI	Personnel Authority
PDD-61 (Feb. 1998)	A new Office of CI (OCI) was created. The Director of the new OCI *will be* [emphasis added] a senior executive from the FBI. The Director of the FBI, along with other officials, including the Director of Central Intelligence, as involved principles, will provide support to the Secretary of Energy in the implementation (of PDD-61) and continuation of an effective CI Program.	Attorney General nominated, at the recommendation of the Director, an FBI SES-level Special Agent to assume OCI leadership. Three OCI leaders from the FBI served under this authority.
Section 3232, National Defense Authorization Act of 2000 (P.L. 106-65). Codified at 50 U.S.C, Section 2422.	Provided statutory basis for separate Office of Intelligence and OCI, both reporting directly to Secretary. Stated that the Director of the FBI *may detail* [emphasis added], any employee of the FBI to the Department for service as Director, OCI. Bifurcated CI Program by establishing a separate Office of Defense Nuclear CI (ODNCI) within the NNSA. Secretary to appoint Dir., ODNCI, *in consultation with* Dir. of the FBI.	Diluted the requirement that the Director, OCI be an official of the FBI. FBI has consultative role in appointment of leader of new NNSA - ODNCI.

Authority	Role of the FBI	Personnel Authority
Section 3117, National Defense Authorization Act of 2007 (P.L. 109-364). Codified at 42 U.S.C., Section 7144(b) note.	Consolidated CI across NNSA and DOE (reversing NDAA of FY2000). Dissolved ODNCI within NNSA, and transferred personnel and functions to DOE CI. Established Intel Executive Committee. CI budgets to be tracked separately, according to that which is requested for CI for NNSA facilities and other DOE facilities.	Amended NNSA Act to reflect that the Secretary of Energy may choose the Director OCI and Director OI from SES, SIS, SNIS, or "any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate." Outside of being part of the Intelligence Community and, therefore, possibly having indirect influence with the DNI, the FBI no longer has any formal statutory role in the recommendation of candidates for the Director, OCI position.