AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# CONTINUING SECURITY CONCERNS AT LOS ALAMOS NATIONAL LABORATORY

## HEARINGS

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JANUARY 30, APRIL 20, 2007

**Serial No. 110–1**

Printed for the use of the Committee on Energy and Commerce

*energycommerce.house.gov*

U.S. GOVERNMENT PRINTING OFFICE

35–446 PDF WASHINGTON : 2007

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) 512–2250 Mail: Stop SSOP, 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
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
DIANA DEGETTE, Colorado
*Vice Chairman*
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA 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

JOE BARTON, Texas
*Ranking Minority Member*
RALPH M. HALL, Texas
J. DENNIS HASTERT, Illinois
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
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE 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, *General Counsel*
SHARON E. DAVIS, *Chief Clerk*
BUD ALBRIGHT, *Minority Staff Director*

---

### SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

BART STUPAK, Michigan, *Chairman*

DIANA DEGETTE, Colorado
CHARLIE MELANCON, Louisiana
HENRY A. WAXMAN, California
GENE GREEN, Texas
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
JAY INSLEE, Washington

ED WHITFIELD, Kentucky
*Ranking Minority Member*
GREG WALDEN, Oregon
MIKE FERGUSON, New Jersey
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

# CONTENTS

## JANUARY 30, 2007


Page

Barton, Hon. Joe, a Representative in Congress from the State of Texas, opening statement ..... 7
Burgess, Hon. Michael C., a Representative in Congress from the State of Texas, opening statement ..... 11
DeGette, Hon. Diana, a Representative in Congress from the State of Colorado, opening statement ..... 8
Dingell, Hon. John D., a Representative in Congress from the State of Michigan, opening statement ..... 5
Green, Hon. Gene, a Representative in Congress from the State of Texas, prepared statement ..... 13
Murphy, Hon. Tim, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement ..... 13
Stupak, Hon. Bart, a Representative in Congress from the State of Michigan, opening statement ..... 1
Walden, Hon. Greg, a Representative in Congress from the State of Oregon, opening statement ..... 10
Whitfield, Hon. Ed, a Representative in Congress from the Commonwealth of Kentucky, opening statement ..... 4


WITNESSES


Anastasio, Michael R., Director, Los Alamos National Laboratory ..... 56
Prepared statement ..... 73
Answers to submittted questions ..... 96
Brian, Danielle, executive director, Project on Government Oversight ..... 19
Prepared statement ..... 98
D'Agostino, Hon. Thomas P., Acting Administrator, National Nuclear Security Administration ..... 51
Prepared statement ..... 111
Friedman, Gregory H., Inspector General, U.S. Department of Energy ..... 15
Prepared statement ..... 119
Podonsky, Glenn S., Chief Health, Safety and Security Officer, Office of Health, Safety and Security, U.S. Department of Energy ..... 17
Prepared statement ..... 132
Pyke, Thomas N. Jr., Chief Information Officer, U.S. Department of Energy ... 55
Prepared statement ..... 143
Sell, Hon. Clay, Deputy Secretary, U.S. Department of Energy ..... 40
Prepared statement ..... 145
Wilbanks, Linda, Chief Information Officer, National Nuclear Security Administration ..... 53
Prepared statement ..... 148


## APRIL 20, 2007


Blackburn, Hon. Marsha, a Representative in Congress from the State of Tennessee, opening statement ..... 164
Burgess, Hon. Michael C., a Representative in Congress from the State of Texas, opening statement ..... 171
DeGette, Hon. Diana, a Representative in Congress from the State of Colorado, prepared statement ..... 166
Dingell, Hon. John D., a Representative in Congress from the State of Michigan, opening statement ..... 161

Page

Doyle, Hon. Mike, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement ..... 170
Green, Hon. Gene, a Representative in Congress from the State of Texas, prepared statement ..... 163
Stupak, Hon. Bart, a Representative in Congress from the State of Michigan, opening statement ..... 157
Walden, Hon. Greg, a Representative in Congress from the State of Oregon, opening statement ..... 162
Whitfield, Hon. Ed, a Representative in Congress from the Commonwealth of Kentucky, opening statement ..... 160

WITNESSES

Anastasio, Michael R., director, Los Alamos National Laboratory, Los Alamos, NM ..... 184
Prepared statement ..... 201
Bodman, Hon. Samuel, Secretary, U.S. Department of Energy ..... 172
Prepared statement ..... 198
Friedman, Hon. Gregory H., Inspector General, U.S. Department of Energy ..... 182
Prepared statement ..... 202

# CONTINUING SECURITY CONCERNS AT LOS ALAMOS NATIONAL LABORATORY

**TUESDAY, JANUARY 30, 2007**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:00 a.m., in room 2123, Rayburn House Office Building, Hon. Bart Stupak (chairman of the subcommittee) presiding.

Present: Representatives Stupak, Degette, Melancon, Green, Dingell [ex officio], Whitfield, Walden, Burgess, Murphy, and Barton [ex officio].

Also present: Representatives Udall of New Mexico and Wilson of New Mexico.

Staff present: John F. Sopko, Christopher Knauer, Voncille T. Hines, Rachel Bleshman, Peter Goodloe, Christopher Treanor, Jodi Seth, Alec Gerlach, Alan Slobodin, Dwight Cates, and Matthew Johnson.

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

Mr. STUPAK. This meeting will come to order on the Energy and Commerce Committee, Subcommittee on Oversight and Investigations. This hearing, which will be the first of the 110th Congress, is entitled, Continuing Security Concerns at Los Alamos National Laboratory.

We will begin with the Members' opening statements.

Los Alamos National Laboratory is a place of great history. It is home to many of our Nation's most secret of weapons development, and yet it is also home to some embarrassing lax security protocols.

During my 12 years on the Oversight and Investigations Subcommittee, I have sat through far too many hearings detailing problem after problem at Los Alamos.

Now as I take over as chairman of this distinguished subcommittee, I find myself presiding over yet another hearing about inadequate security at the lab. The latest security debacle begins in October 2006 when Los Alamos County Police responded to a call at a private residence and discovered several hundred pages of classified and unclassified materials as well as electronic files that were stolen from the Los Alamos National Laboratory.

Documents were taken from the lab by a subcontract employee. The employee simply walked out of the lab with stolen documents

in her purse or on a thumb drive which she easily inserted into open ports on classified computers.

Over the last 8 years, this subcommittee has held 11 hearings into various security lapses at Los Alamos. I have this chart which I will enter into the official record illustrating 11 hearings that this committee has held. These hearings have ranged from the Wen Ho Lee case in 1999 to the removal of Classified Removable Electronic Media, CREM, in 2005 in the cyber security hearings we held in June 2006.

Throughout these hearings, Members have heard time and again how the Department of Energy and the lab managers were going to improve security. We have heard excuse after excuse and plan after plan of how the lab would improve security. The DOE went so far as to competitively bid out the lab's operation in the hope that a new management team would bring about change, security and accountability.

But DOE awarded the contract to a consortium that includes the previous contractor, the University of California. With this brilliant decision, did anyone really expect the laissez faire culture of Los Alamos to change?

As a result of our investigation, I have a number of questions that need to be answered today. How and why did the October security breach occur? What is the potential and overall actual harm to national security as a result of the breach? Why do security breaches continue to plague Los Alamos? What plans do Los Alamos, DOE and the National Nuclear Security Administration have for preventing breaches at Los Alamos? Who is accountable for the most recent security breach at Los Alamos? What tools are available to the Federal Government to hold Los Alamos accountable for the latest security breach?

For example, new accountability rules allow DOE to penalize contractors and their subcontractors for violations of DOE rules, regulations and orders regarding the safeguarding of restricted data and other classified information. Based upon our staff's investigation, my real concern here is whether DOE is using these tools, or is it just giving contractors a slap on the wrist for egregious security violations? Are the tools available for the Federal Government to adequately deter security breaches? This incident does raise serious questions about the manner and policies of the Department of Energy in granting the security clearances to employees. This question, as well as many others, will of course have to be answered in closed session due to their sensitivity.

During the last hearing in 2006, I became so fed up that I asked the question, "What do we do at Los Alamos that could not be done at our other National Laboratories?" I was serious when I asked that question back then, and I must tell you I have been asking myself the same question again in recent months.

I am a former police officer, and in Michigan, we like to use auto analogies. For far too long we have essentially been issuing parking tickets to Los Alamos. In July 2004, we essentially put a boot on the lab when it was shut down for 7 months to clean up its act. This cost the American taxpayers more than $350 million and was supposed to result in a more secure facility. Unfortunately, there has been yet another breach not long after Los Alamos reopened.

Los Alamos did not change after repeated tickets. It did not change after putting a boot on. And now, I am convinced that we may need just to tow the car.

Something drastic must be done at Los Alamos in order to change the systemic security problems. The American people demand and deserve the highest level of protection of our national secrets. If the Department and the lab won't change, provide security at our labs, Congress must explore ways to protect our security. Therefore I will, in cooperation with my friends on the minority side, be asking the Government Accountability Office to perform a comprehensive audit of all services performed at Los Alamos.

I will ask them to evaluate whether the footprint and mission at the lab is too large.

I will also ask them to evaluate the possibility of consolidating and moving many of the classified operations at Los Alamos to another lab, such as Sandia where there is a willingness among the employees and management to heed our advice. I will not tolerate continued security lapses and thumbing of their nose at Congress.

Finally, it is my understanding that Secretary Bodman has asked for additional reviews of Los Alamos's security and that the reports of the review are due at the end of February. It is our expectation that the Department will take these reviews seriously, provide concrete answers and submit detailed plans to remedy the security lapses.

I fully expect Secretary Bodman will appear before this subcommittee to articulate what has and will be done to improve security at Los Alamos.

In conclusion, I am pleased that the first hearing of the O&I Committee is truly a bipartisan effort by myself, the ranking member and our staffs. This is what I hope will be the first of many bipartisan efforts to make our country safer and our government more effective.

Thoughtful and tough oversight is neither Republican nor Democratic. It is just good government. I salute the former chairman and his staff for all their work in this inquiry. I look forward to continuing to work with him.

The Constitution entrusted Congress with a solemn duty to oversee the activities of the executive branch. Oversight is the only way Congress can assure that our laws are adequately and properly administered.

Without effective oversight, how can Members of Congress truly determine with confidence what additional laws are needed? As chairman of the subcommittee, I plan to be persistent in our oversight responsibilities, fully realizing that Congress's power to probe is a necessary tool of our democracy that is best wielded in a nonpartisan manner.

Again, I want to thank our former chairman, the gentleman from Kentucky. I look forward to working with all the members of the committee and the Subcommittee on Oversight and Investigations. With that, I would yield to Mr. Whitfield.

**OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY**

Mr. WHITFIELD. Mr Chairman, thank you so much for holding this important hearing, and I certainly want to congratulate you on your new with your new responsibilities as chairman of this subcommittee.

As you said, we have held several hearings to review ongoing security problems at Los Alamos over the last 3 or 4 years.

And as long as it is important that we continue to do, so I am delighted that we are continuing to hold these hearings.

Prior investigations led by this subcommittee have uncovered the details of the 1999 Wen Ho Lee case, the 2000 NEST team hard drive incident, and several incidents in 2003 and 2004 relating to the improper handling and destruction of classified removable electronic media, and then, in 2004, operations at Los Alamos were shut down for a 6-month period in an attempt to deal with many of these problems.

At each subcommittee hearing, Los Alamos officials have promised to solve ongoing security problems.

But they have failed to follow through.

I was pleased when the Department recently decided to compete the Los Alamos contract for the first time in over 60 years.

In June 2006, a new consortium named, Los Alamos National Security began operations at its site. In its contract, LANS has made several commitments to solve the security problems at Los Alamos. Unfortunately for LANS, only 4 months passed before the most recent security incident occurred. In October 2006, it was discovered that 1,588 pages of classified documents from a classified vault had been removed in paper form and also downloaded on to a portable thumb drive. The documents and the thumb drive showed up in the trailer home of a former LANL employee.

Now, 1,588 pages—I just want to show you, this is 1,588 pages. So it is really quite shocking that this is still going on in this magnitude.

However unfortunate the time, LANS must be held accountable for compromising these documents, and it should pay a price. This incident demonstrates that the Department and LANS have failed to implement an effective security policy at Los Alamos.

DOE must assert its contract and regulatory authorities to compel greater security performance.

This most recent security incident demonstrates the same poor security management, lack of formality of operations, and insufficient oversight that has plagued the lab for decades. I do not think the security problems at Los Alamos can be solved with small changes on the margin.

Dramatic, new ideas from the Department, from LANS and from Congress, are needed.

I have co-signed legislation drafted by Mr. Barton to strip NNSA of its autonomy with respect to safeguards and security, worker health and safety and cyber security oversight, and understand that Chairman Dingell and Chairman Stupak have also cosponsored this important legislation. I would also note that we signed a co-letter last night along with Mr. Barton and Representative

Hastert that asked the Department to take immediate steps to solve the security problems at Los Alamos.

The letter has several recommendations and urges DOE to take action to reduce the volume of classified material across the laboratory. At Los Alamos, operations are spread out over a 43-square mile area. The lab has approximately 15,000 employees, 3,000 classified computers and 1,774 classified security areas. To give you some perspective, there are more classified security areas at Los Alamos than there are total rooms in the Rayburn, Cannon and Longworth House Office Buildings combined.

And at this time, I would ask unanimous consent to introduce into the record the letter that we just referred to, that we had sent. Do they have a copy of it?

Mr. STUPAK. Without objection, it will be part of the record.

Mr. WHITFIELD. LANL's volume of classified holdings is unnecessarily large, conducted in too many security areas and involves too many people. These factors, including the geographical dispersions of activities, make LANL susceptible to security failures. I hope this subcommittee can help identify the right solutions to fix this problem once and for all. Thank you.

Mr. STUPAK. I thank the gentleman from Kentucky.

Next, the gentleman from Michigan, chairman of the full Energy and Commerce Committee, Mr. Dingell.

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

The CHAIRMAN. Mr. Chairman, first, thank you for recognizing me, and second, congratulations to you on your becoming chairman of this subcommittee. You will do an outstanding job. You have been a superb member of the committee and superb ranking member, and I am delighted to see you sitting where you are.

I want to also say, express my good wishes to the gentleman, Mr. Whitfield, who was so gracious and kind in his conduct in this subcommittee. We look forward to working with him, as I know we all do.

I feel a little bit like this is the movie "Groundhog Day". All of us will remember that we seem to be waking up each morning to repeat the same events over and over with regard to security at the National Laboratories.

As I recall, when the House turned in 1994, this subcommittee was preparing a set of hearings to go into the conduct of matters at DOE and how things were being done at that time with regard to the laboratories.

There were all matters of difficulties, and I won't belabor the matter or delay the process by talking about it.

But the events there with regard to security, security breaches at Los Alamos and the other laboratories, were very serious.

And so I am reminded of what Yogi Berra used to say, this is like deja vu all over again. I am somewhat distressed that this subcommittee must convene to hear about security breaches at the National Energy Labs, Los Alamos in particular. We could drag out stacks of letters sent to the Department Secretaries and the Presidents over the past two decades on the issue we are reviewing

today. We could also display a small tower of hearing records, many of which I chaired, relating to security breakdowns at DOE and at the Los Alamos National Laboratory in specific.

This would be good drama in a movie. These, however, are security breaches and are deadly serious. They threaten our security to guard our Nation's military secrets, our nuclear secrets and other matters of importance. For some reason or another, DOE has proven itself incapable of managing this critical security and preventing recurring problems that we will discuss today.

There is a new twist to this story, and I find it a worrisome development. Apparently, this latest security breach raises serious questions about DOE's process and procedures in granting security clearances and the adjudication of adverse information dealing with the suitability of employees and contractors.

This appears to be, in part at least, a new issue. And it should be the subject—as it is going to be—of an executive session which is going to take place later today. We may very well need to expand the investigation of this subcommittee into DOE's personnel security system.

Mr. Chairman, it is our joint concern that we will hear the same promises that we have heard in the past about how DOE will remedy the situation, how this lab is now going to take security matters seriously and how the lab will be reorganized, how some officers and officials and managers may be removed.

I must confess that I have been hearing these promises for a long time, and I am beginning to find them somewhat tedious. The time has come to focus on the adequacy of the tools DOE possesses to effectively penalize the contractors and the lab for serious security failures, and whether DOE ever intends to use them or knows how to do so. There may be nothing in the Secretary's toolbox effective enough to turn this lab around. We will need to determine that in today's hearing and to find whether penalties are sufficient to effectively improve security at Los Alamos.

I understand that Secretary Bodman, for whom I have considerable affection, is considering yet another security review regarding Los Alamos specifically and the Department in general. I look forward to his appearance before this subcommittee in February to learn what he intends to do to fix this mess. I support requesting the Government Accountability Office to conduct a comprehensive audit of Los Alamos operations in order to determine what functions need to be retained, there versus being moved to another government or private facility.

It increasingly appears that the overall footprint of the lab may be too big in both physical scale and in the scope of its mission to be properly managed.

At this point, all options should be open, on the table for consideration as to how we correct this intolerable situation.

Again, Mr. Chairman, congratulations. Thank you for holding this hearing, and I look forward to hearing what will be said by our witnesses. But I hope you will forgive me, as I note in the case of Groundhog Day, we have seen all of this before.

Thank you Mr. Chairman.

Mr. STUPAK. I thank the gentleman.

Next turn to the distinguished former chairman of the full committee, Mr. Barton of Texas.

**OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS**

Mr. BARTON. Thank you, Mr. Chairman. I, too, want to congratulate you on the assumption of your new duties as the subcommittee chairman of Oversight and Investigations. I consider this subcommittee to be the heart of the full Energy and Commerce Committee.

You are following in some big footsteps; in the prior Congress, Mr. Whitfield, but if you want to go back to when your party was last in the majority, the full committee chairman, Mr. Dingell, was also the subcommittee chairman, and this is where he gained his reputation for making sure that the ship of state was sailed straight.

So, we are going to have a good relationship.

I want to echo what Mr. Dingell just said, if there is nothing else to do on the Oversight and Investigation Subcommittee it seems you can also hold a hearing of security lapses at Los Alamos.

I believe this is the 10th hearing in the last 4 years. I could be wrong about that. But I wouldn't be off by much; 2004 the entire laboratory complex was shut down for 7 months; 2005, 1,500 records—including Social Security numbers—some people hacked into the system, stole those numbers and the Administrator didn't even bother to tell the Secretary of Energy about it.

This last October, approximately 1,600 documents were stolen and carried out of the complex and, if my memory is correct, were found in a mobile home when the local police responded to a domestic disturbance.

Enough is enough.

This is not a fast food restaurant on the corner somewhere. This is the crown jewel of our weapons complex.

I don't have words to explain how frustrated I am, and I think my frustration is shared by every member of the committee.

I am happy to report that last evening we introduced a bipartisan bill, Mr. Stupak and Mr. Dingell, original cosponsors, along with myself, Mr. Whitfield and Mr. Hastert, that strips the NNSA of its authority to manage some of these problems and gives it back to the Secretary of Energy to delegate as he sees fit. It is H.R. 703.

And I hope that bill is given a hearing very quickly at subcommittee, or perhaps even at full committee and is moved to the floor. We need to do something about this problem.

If there were a way to start over, I would say, shut down Los Alamos, fire everybody out there and build a new weapons laboratory somewhere else. That is not cost-effective. And obviously, there are many, many good people at the laboratory. But there is an absolute inability or unwillingness to address the most routine security issues at this laboratory.

I have sent a letter to the Secretary of Energy, Mr. Bodman, today making him aware of this new legislation. But I have also asked him to immediately consider doing the following things by his authority as the senior executive officer of the Department of Energy. I have asked that he consider directing the Office of

Health Safety and Security to conduct an immediate inspection at Los Alamos and to repeat it next 2 years to report any problems and report any progress in security and worker safety.

I have asked the Secretary to consider directing Los Alamos to dramatically reduce and consolidate the number of classified activities, the number of classified computers, the number of classified vaults. They have got classified material strewn all around the complex. I have visited Los Alamos, seen for myself some of these sites where they store classified material. I am not an expert on security, but I consider the current number of sites to be many, many more than is absolutely necessary. And one simple solution to the problem would be just to reduce the number of places they keep this material.

I also think that the current contractor at Los Alamos apparently doesn't give a damn about this. And I hate to use that kind of language, but that is the way I feel.

If it is contractually legal, I think part of their fee should be withheld, perhaps even forfeited. If the contract allows for civil penalties I would hope the Secretary would consider assessing those penalties. If you can't get somebody's attention any other way, sometimes you can get their attention by withholding financial assets.

So it is obvious that we are not going to solve this problem with one hearing, Mr. Chairman. But I do want to commend you for being willing in your first hearing of all the things you could do, to tackle this issue. It is a very serious issue. And I will pledge to you that the minority is doing to continue to work on this problem. And now that you are the chairman and Mr. Dingell is a full committee chairman, you will have our full cooperation in trying to get on the bottom of it and rectify the situation if it is possible. And if it is not, if after a year or year and a half, if it doesn't look like any progress is being made, I do reserve the right to request that we consider shutting down this laboratory.

If that is the only way to do it, and we have to start over, then so be it.

But we ought to be able to get security right at Los Alamos.

With that, I yield back.

Mr. STUPAK. I thank the gentleman, and we do anticipate at least one more hearing on this subject with Secretary Bodman probably in March. And with that, I would yield to the distinguished vice chair of the full committee, Ms. DeGette of Colorado.

**OPENING STATMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO**

Ms. DEGETTE. Thank you very much, Mr. Chairman. It is good to see you in that chair after all these years working with you on this subcommittee, which I consider to be the best subcommittee in the House.

And I also want to add my congratulations to the new vice chairman of the subcommittee, Mr. Melancon. He is going to have a great time.

One thing that is so great about this subcommittee is, when we get mad, we get really mad in a bipartisan way. And I want to echo

what former chairman Barton said, because I have been on this subcommittee during my 10 years in Congress, and you are exactly right, we have had about six to 10 hearings in the last few years alone on this subject. And we have been told repeatedly in every single hearing that this problem would be fixed.

In 2004, then-Chairman Barton and I visited Los Alamos, and this was akin to a state visit for Los Alamos I guess. We went in; there was tremendous local interest. There was tremendous, tremendous effort to brief us and show us what was going on. The deputy secretary was there. The new director was there. Everybody was there. We toured the facility. We had some very tough conversations. We were told that this situation was going to be fixed and that this situation was going to be fixed immediately.

And subsequently, that director who was with us was drummed out, and nothing happened, as we have new seen. Mr. Dingell talked about Groundhog Day, and this week, in fact, is Groundhog Day, so it is appropriate that we are having these hearings this week, but it is not funny about these security breaches. The lab is home to some of the most confidential and important data in the Nation, weapons development, security of our nuclear stockpile, the development of technology to protect us from terrorist attacks. And it is not the first time either that we seem to be dependent on dumb luck to discover a breach of security.

If it hadn't been for the vigilance of police officers in investigating unrelated drug charges, this classified data would still be sitting at the home of a former subcontractor for a yet to be discovered purpose. And so, really, the issue is so much broader than just this single incident.

And as we will hear today, the Department of Energy's Inspector General recently found that physical and cyber security at the lab have been consistently compromised. We keep saying to ourselves, why does this happen time after time, year after year? And we haul everybody in, and we rant and rave, and then it happens again.

I think there are two problems. There is the oft discussed culture at Los Alamos where people really think themselves beyond the requirements of true security measures. But there is another problem, and former chairman Barton alluded to this. It is such a large site and with so many different areas that contain this data, that it is very difficult to secure it.

And in addition, when I visited, I found, 3 years ago, some of the security measures being implemented would be just routine security measures at a private facility, and so you have got to wonder, do these Government facilities think that they have to comply with lower standards than in private industry? So, really, I think the questions that former Chairman Barton and Chairman Stupak and Chairman Dingell are asking are the right questions.

And I cannot stress enough to the witnesses today and to those who care about this facility, we are really serious and we are really serious this time, I think the legislation that was introduced is drastic, but that is the direction we are going to have to go unless we can get some clear answers of how we are going to fix this problem.

With that, Mr. Chairman, I yield back.

Mr. STUPAK. Before the gentle lady leaves, if we can do housekeeping. I notice there is a majority of the committee present, and we are going to have to take a vote to move into classified or executive session later. We won't do it—so before we continue, all those in favor of moving to an executive session later, please just raise your hand or indicate aye.

Any opposition? Hearing none, at the appropriate time, we will move into executive session later in this hearing. With that, we will continue with the opening statements, next turning to Mr. Walden.

**OPENNG STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON**

Mr. WALDEN. Thank you, very much, Mr. Chairman, and I think people who have come before me have laid it out pretty clearly and forcefully. There are just few things as important to our Nation's security as maintaining the security of our classified data in our National Labs. I think my colleagues have made that clear. You have heard it from me before in these hearings we have had in the past. The chairman said, these are the crown jewels of our weapons systems. And I guess what strikes me is, we have got employees who still are walking out the front door with the diamonds out of the crown jewel set. And that is a problem. That is a very serious problem and one that this subcommittee has railed on before in public and in private sessions, perhaps even more so than what people are hearing in the public session. There are some fundamental questions that we will have for all of you today that will come in both sessions, including access to these computers once again, how is that controlled, how does somebody walk out with a thumb drive? I understand you are now using a product like this, J-B Weld, the world's finest cold weld, to actually seal up the USB and FireWire ports so that somebody can't use one of these thumb devices.

It is great. It works for engine blocks, and it works for faucets, and I guess it works to plug leaks in our national security system, too, but why do we even order computers that have those ports in them? It would seem to me that Government could work out a contract to get a computer that doesn't have them. I am glad you now sealed up 7,200 of these ports or whatever the actual count is. Perhaps we will learn later today. But it strikes me as a bit strange that we are relying on J-B Welds to protect leaks of our national security.

With that, Mr. Chairman, I will yield back.

Mr. STUPAK. I thank the gentleman. Next, I turn to the vice chair of the subcommittee, Mr. Melancon.

Mr. MELANCON. Thank you, Mr. Chairman. I don't have any written statements. I would like to move as quickly as we can into testimony.

Being new on the committee and just picking up the gist of what has been said about Los Alamos, and in looking at the concerns that we have about nuclear proliferation around the world, and we are not even protecting our own, it seems so. With that, I'd just like to thank you for allowing me to be part of the committee and the ranking member and the members of the committee. Thank you.

Mr. STUPAK. Thank the gentleman.

Next, I turn to Mr. Burgess, Dr. Burgess.

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

Mr. BURGESS. Thank you, Chairman Stupak and Ranking Member Whitfield for continuing this committee's important oversight over Los Alamos. Chairman Stupak, I appreciate the bipartisan nature of this hearing, and I hope it is a sign of how you will handle hearings in the months to come. You and your staff are to be commended for your preparation and your willingness to share relevant information with members across the aisle.

Mr. Chairman, it is my sincere hope that we have your commitment to continue this collegial and bipartisan disposition throughout all the hearings of this congress. And I would also like to take a minute and thank Ranking Member Whitfield for his investigation of Los Alamos throughout the years. Clearly, today's hearing builds upon the hard work and the determination that you and your staff have displayed on this crucial matter of national security. I thank you for your leadership on this important issue.

Today we have three panels before us that will hopefully be able to explain to us not only what exactly happened in October but also what has been done to prevent another recurrence. I welcome you all here today and hope we can get to the bottom of this continuing problem at Los Alamos once and for all. I would especially like to welcome my fellow Texan, Deputy Secretary Clay Sell. Thank you for being here with us today and sharing your valuable insight into the Department of Energy.

In the post–9/11 world in which we live today, our national security has become the most important issue facing our Nation. We must do everything within our power to ensure that we do not become the victims of terrorism again. As terrorists become more and more sophisticated, we must continue to implement and maintain comprehensive measures to secure our safety. While we often think of terrorists of being from foreign lands, it is easily plausible that people living on American soil can compromise our country's national security interests. The fact that someone can walk out of an institution that developed the atomic bomb with a disk full of classified information is deeply disturbing. This is absolutely indefensible.

Los Alamos has some of the smartest minds, people of almost immeasurable brilliance, working on the facility, and the reoccurrence of so many security breaches is simply inexcusable. I was taught that people should be held accountable for their actions. While there are many organizational changes that can be made to better ensure the security of our country's classified information, one of the easiest and most effective remedies is to make the contractor in charge of security pay a step penalty. As a steward of the taxpayer dollar, I fully support this idea. If the contractor is penalized, millions upon millions of dollars maybe, then they will finally realize how serious the problem is and that it must be stopped.

While there is clearly an institutional problem at Los Alamos, we must also remember that there are thousands, 15,000, hardworking employees at the lab who make a remarkable contribution to science in this country on a daily basis. I had the pleasure—the

honor of visiting the lab in July 2005, and I met many of those hardworking and dedicated men and women. I was impressed by their dedication. I was impressed by the overall intellect of the individuals involved.

In preparation for this hearing, I came across a posting on a well known blog of Los Alamos employees. The posting was addressed to members of this committee and ended with this thought: "Don't give up on us just yet. Please be careful with your words. Direct them at those who are truly at fault and avoid belittling comments directed against the whole workforce and against the vital work that we can do to help this country. And one more thing, yes, you do need Los Alamos—a well functioning Los Alamos".

I completely agree with this employee. The country needs a well functioning Los Alamos. And that is why we are here today, to protect what is a national treasure.

And I would oppose any diminution of that mission or relocation of the resources, but oversight is our obligation.

Mr. Chairman, I have several questions that I hope we will get answered, and one of those questions deals with the RFP process that the lab went through just a little over a year ago. Was it a fair process? Was the University and the contractor that was not selected, were they given a fair shake? Were they given a fair chance to compete for that contract?

It seems as if the embedded culture at Los Alamos is incapable of change. Perhaps that is reason enough that we should reopen the RFP process.

Mr. Chairman, I again thank you for the bipartisan hearing in which we can further address this troubling issue and what needs to be accomplished with this dismal and depressing cycle of security breaches at Los Alamos.

And I feel it is important that we continue to work on this problem so that we do not risk the welfare of our Nation and succeeding generations who will either benefit from our decisions or inherit the failings of our security lapses. With that, I will yield back.

Mr. STUPAK. I thank the gentleman.

The gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman, and I am glad to be back on the subcommittee although following our chairman, when it is his deja vu, I have been off this subcommittee for I think three terms, and it seems like we ended and that last term with Los Alamos obviously back then much more serious allegations than we have today.

But, Mr. Chairman, I have a statement I would like to place into the record and express the same frustration I think everyone has heard on a bipartisan basis, but I would like for us to get moving and see what we can do. But also I am thankful that we have local law enforcement who were sharp enough to pick that up, but hopefully we can stop it before it actually leaves the lab. With that I will submit my statement for the record and yield back.

[The prepared statement of Mr. Green follows:]

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

Mr. Chairman, I am privileged to be back on the Oversight Subcommittee, but it looks like not a whole lot has changed, we are still looking into security problems at Los Alamos.

Everyone up here and all our witnesses are upset, but I do not think anyone has made the point that since our intelligence overseas has not been as good as it could be, we cannot afford nuclear security mistakes here at home.

The risk of international nuclear proliferation is bad enough with Iran and North Korea without having to worry about risks in our own backyard.

Some members of this committee criticized the previous administration for security lapses that occurred in the years after the cold war and rightfully so.

But now, more than 5 years after 9/11, this administration has still not resolved many of the same issues. It looks like 9/11 led to increased security everywhere but Los Alamos.

The National Nuclear Security Administration imposed millions in financial penalties against the University of California for problems at Los Alamos in past years, and the new contractor could be liable for even larger penalties.

I notice that we have some new faces in charge, and some former officials are pursuing other opportunities. I certainly hope the changes are noticed on the ground as well.

However, I have to say I am somewhat bothered by much of the testimony here today.

The testimony contains lots of findings from internal investigations and a great deal of new and updated directives and procedures.

We've heard this same song about security breaches before-with similar findings of root causes and similar new procedures. In fact, DOE and Los Alamos just keep re-releasing the same album.

Instead of more studies and procedures, I think the problem may be a lack of actual leadership and people who will implement the procedures in a coherent way.

So I hope our new faces here are not just interested in more studies, more investigations, and more new set of rules.

Instead I hope they and their managers get out there and work with the subcontractors, security personnel, scientists, and employees and change the situation on the ground.

Hopefully Congress does not have to remind the administration that several countries opposed to the United States are currently seeking nuclear weapons.

We need to keep our technologies out of these nations' hand and we need to be dead serious about it.

Thank you Mr. Chairman and I yield back.

Mr. STUPAK. Without objection, and welcome the gentleman back to this subcommittee.

Mr. Murphy from Pennsylvania, any opening statement?

## OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Thank you, Mr. Chairman, and it is a pleasure to be joining you on this committee. Mr. Chairman we are about to hear about these appalling violations and blatant disregard to national security safeguards at Los Alamos National Laboratory, and they warrant intense scrutiny of this facility. The unauthorized removal of any classified materials is, of course, a grave matter. But the frequency at which classified materials seem to be removed at Los Alamos National Laboratory indicates a careless attitude towards our national security and deserves the intense scrutiny of this committee.

One such display of this disregard for national security occurred in 2005, as referenced by the members here, when the former administrator of the National Nuclear Security Administration Linton Brooks—for 9 months, Administrator Brooks refused to report com-

puter hackers' theft of 1,500 Social Security numbers and personal information of employees of the NNSA. Another instance, in October 2006, we know police found a flash drive and hundreds of pages of classified documents at the home of a former subcontractor, the content of which is so classified it can't be released to the public, but nonetheless it raises our concerns deeply.

For the sake of our national security, we must determine how they were removed and take immediate steps to prevent this from occurring in the future. We need to prevent breaches through better security systems on computers and hardware, to thoroughly screen everyone, especially contractors at Los Alamos, to fully inspect those materials that come in and out of the facility, and to prosecute to the fullest extent of the law and give stern penalties for those who breach that security.

As our society is growing more dependent on technology, we have seen a disturbing trend in the theft or loss of personal information from Government agencies, such as the VA and large corporations, that at times are used for malicious intent.

What has been the consequence of the theft of this material and who is responsible for their loss or misuse? We need answers to these questions, and we need ideas on how to prevent this in the future.

Misuse of personal information must have consequences. For example, in the 109th Congress, I introduced the SERVE Act which would physically secure all sensitive personal information and all equipment containing such information processed and maintained by the Department of Veterans' Affairs. But I also would have also required the VA and its contractors to encrypt sensitive personal information. The SERVE Act also imposed criminal penalties for unauthorized disclosure of sensitive personal information.

But we are here not to address just one or two of these problems but to find a way to address a chronic failure to follow national security procedures in guarding classified materials. I look forward to this hearing, and I yield back.

Mr. STUPAK. I thank the gentleman. We should note that Mr. Udall is here. He is not a member of the committee, but Los Alamos is in his district. He is very concerned about it and has always been a strong advocate for Los Alamos. You can see the concerns of members, Tom, but welcome, and I look forward.

Mr. UDALL. Thank you and a pleasure to join you today, Mr. Chairman. Thank you.

Mr. STUPAK. We are in recess until noon so we should be able to get hopefully most of this hearing in. It is the policy of the subcommittee to take all testimony under oath.

Please be advised that witnesses have the rights under the Rules of the House of Representatives to be advised by counsel during their testimony.

Do you desire to be advised by counsel at this time? If so, please introduce your counsel. Seeing no reaction, I advise, we do swear in witnesses. Would you please rise and raise your right hand?

[Witnesses sworn.]

Mr. STUPAK. Let the of record state an affirmative response of the witnesses. Witnesses are now under oath. You have 5 minutes for an opening statement. Witnesses may, at the discretion of the

committee, submit brief and pertinent sworn statements for inclusion in the hearing record.

Let me now start with Mr. Friedman please.

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

Mr. FRIEDMAN. Mr. Chairman and members of the subcommittee, I am pleased to be here at your request to testify on the Office of Inspector General's review of the recent compromise of classified data at the Department of Energy Los Alamos National Laboratory. Los Alamos, as has been stated earlier today, has been at the forefront of our Nation's security related research and development enterprise for over 60 years. There have been a number of highly publicized incidences that have cast doubt on the laboratory's ability to protect national security.

The Office of Inspector General has performed numerous audits, inspections and investigations of physical, and cyber security related issues at the laboratory.

Our reviews have covered diverse areas such as the implementation of design bases threat, safe guards over classified material and property and security of information systems. I have been asked to testify before this subcommittee and other congressional panels on several occasions regarding management of security interest issues at Los Alamos.

No doubt the subcommittee is fully aware of the circumstances surrounding the recent seizure of classified information from a residence by the Los Alamos county police department. Shortly after the material was seized, Secretary Bodman requested that the Office of Inspector General begin a review of the compromise of classified data.

The Secretary also asked that we evaluate certain aspects of the Department's security clearance process, the results of which can be discussed in closed session.

Our special inquiry disclosed that, despite the expenditure of tens of millions of dollars by the National Nuclear Security Administration to upgrade various components of the laboratory security apparatus, the security environment was inadequate.

Specifically, our special inquiry revealed that, first, certain computer ports which could have been used inappropriately to migrate information from classified systems to unclassified devices and computers had not been disabled.

Second, classified computer racks were not locked.

Third, certain individuals were inappropriately granted access to classified computers and equipment to which they were not entitled.

Fourth, computers and peripherals that could have been used to compromise network security were introduced into a classified computing environment without approval, and finally critical security functions had not been adequately separated, essentially permitting systems administrators to supervise themselves when it came to security and to override controls.

In many instances, laboratory management and staff had not developed policies necessary to protect classified information, had not enforced existing safeguards or had not provided the emphasis nec-

essary to ensure protective measures were adequate. Some of the security policies were conflicting or applied inconsistently. Also, both laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and inspections. Our findings raised concerns about the laboratory's ability to protect both classified and sensitive information.

The picture before you right now depicts the rack of classified computers at Los Alamos from which the diverted classified information originated. As you can see, the rack that held the computers was unlocked, a condition that permitted access and exploitation of the open ports. And I know you all are familiar—this is a thumb drive similar to the one which in fact was used to divert the material from the laboratory. This is a 1 gigabyte thumb drive, and this can contain the equivalent of two file cabinets full of information to show you how powerful this little item is.

Any diversion of classified material creates a potentially serious national security situation. The full extent of the damage related to the removal of classified information in this case may never be fully known. A criminal investigation of this matter by the FBI continues.

We made a number of recommendations to correct identified deficiencies.

For example, we recommended the Department take immediate action to disable unneeded computer ports, secure classified computer racks, segregate critical security functions and limit classified computer access and privileges to those who specifically require it.

In response to our report, Secretary of Bodman established two high-level task forces to address our findings, and Deputy Secretary Sell directed an immediate review of policies and practices related to computer ports in each of the Department's facilities.

The subcommittee requested that we identify other actions that could improve security at the laboratory. In short, we concluded that the Department should first establish an up-to-date, unified, coherent, risk-based security policy that flows throughout all elements of the Department. It is essential this policy be applied consistently and that all aspects of security, physical, cyber and personnel be integrated to ensure a seamless system.

Second, the Department should aggressively hold individuals and institutions at both the Federal and contractor levels accountable for failure to follow established security policies. Penalties should include meaningful reductions in contractor fees, personnel reassignments and terminations, civil penalties, program redirection and ultimately—should it be needed—contract termination.

One final note, one of the most disturbing aspects of this event is the fact that it was not discovered by the laboratory but by local police during an offsite investigation unrelated to laboratory activities. Without this inadvertent discovery, the diversion of classified material may never have been disclosed. And in that light, the Department and Los Alamos need to strengthen efforts to proactively detect and prevent security breakdowns. This might include, for instance, first improving the level of monitoring of classified computer use through the application of specialized software which is currently available; two, enhancing computer activity logging; and

three, initiating a program of unannounced security checks beyond routine inspections.

Admittedly there is a cost involved with such undertakings, but it is a cost that may be necessary given the pattern of security issues that we have seen at the laboratory.

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

[The prepared statement of Mr. Friedman follows appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you, Mr. Friedman, and I should have properly introduced you as the Inspector General for the Department of Energy. I appreciate your work.

Mr. Podonsky is the chief health safety and security officer at the U.S. Department of Energy.

Mr. Podonsky, your opening statement please.

**TESTIMONY OF GLENN PODONSKY, CHIEF HEALTH, SAFETY, AND SECURITY OFFICER, OFFICE OF HEALTH, SAFETY, AND SECURITY, U.S. DEPARTMENT OF ENERGY**

Mr. PODONSKY. Thank you, Mr. Chairman, and Mr. Whitfield, and members of the subcommittee, I appreciate the opportunity to testify today regarding the improper removal of classified information from the Los Alamos National Laboratory.

At the time of this incident, when it was discovered, our Office of Independent Oversight was conducting scheduled inspections at the laboratory's security, cyber security and emergency management programs.

As we heard from my colleague, Mr. Friedman, his office conducted the inquiry into the circumstances surrounding the incident.

Therefore, I will focus my remarks on our inspection of the laboratory in terms appropriate for this unclassified hearing. Our independent oversight inspection just completed resulted in the lowest set of performance ratings for security and emergency management topics that we have seen at Los Alamos since 1999.

That, combined with the history of security problems at Los Alamos, is of great concern to everyone.

However, these ratings should not leave this committee to conclude that the laboratory is not protecting their most important national security asset. This inspection concluded that special nuclear material, an area with historically significant weakness, is adequately protected.

Additionally, the ratings in part reflect the fact that our independent oversight inspection process has become more technically enhanced and increasingly focused on performance-protection-based activities, especially in the area of cyber security and protection of classified matter.

We note some improvements. However, we continue to conclude that extensive work remains to ensure that Los Alamos fully meets Department's expectations. While special nuclear materials were adequately protected and overall performance of the protective force was considered effective, we identified a number of significant problems with the protection of classified documents and materials and with the configuration of vault-type rooms. It was evident that the site is overly dependent on the use of nonstandard storage con-

figurations for the protection of many of its classified weapons parts. Compensatory measures, established to support approval of the nonstandard storage configurations, were found to be inconsistent and not performing according to plans.

The overall impact of the deficiencies related to the protection of classified matter is substantial.

Also, while some cyber security enhancements have been made, the laboratory's cyber security policies are not comprehensive and not up-to-date with DOE and NNSA requirements, and they do not sufficiently address threats posed by emerging technologies.

Additionally, risk management processes are insufficient, resulting in risk acceptance decisions being made by lower staff members, which is inappropriate.

In many cases, the protection of classified systems is overly dependent on administrator controls to mitigate potential insider activity rather than more robust controls and barriers. As a result, Los Alamos National Laboratory systems continue to operate at increased risk from malicious insiders intent on subverting established departmental requirements.

Another area of concern is the certification and accreditation of both classified and unclassified information systems. The Los Alamos certification and accreditation process has not kept up with current methodologies, and existing processes do not ensure a consistent approach for applying testing necessary security controls. For example over 25,000 existing unclassified work stations in service at Los Alamos were not certified and accredited. Self assessment processes are weak, and very few systems actually are being tested as part of these assessments.

Moreover, deficiencies identified during self-assessments are not always reported to the Los Alamos site office or NNSA, and development of corrective action plans to address them seems to be optional. Consequently, there is little in-depth understanding of program weaknesses. Considering the progress made to date balanced against the cyber security issues that remain, we conclude that strong and aggressive management action is required.

There does need to be sound new laboratory plans for conducting self-assessments and implementing a contractor performance assurance program as part of the contract transition. However, the plans are not yet fully implemented.

In addition, the laboratory does not have an effective process for identifying actions for identified deficiencies. Similarly, the NNSA site office security survey program is inadequate. In a few cases, the laboratory has decided not to comply with departmental requirements, and the laboratory and NNSA did not utilize the Department's mandated deviation process to fully assess and accept risks associated with these decisions.

The recent inspection results illustrate some improvement. However, the most important national security asset at Los Alamos must be recognized to be protected, and that is the special nuclear material.

Nevertheless, significant and disturbing protection and emergency management program deficiencies continue to exist at Los Alamos that require prompt attention, forceful and sustained management actions, and corrective actions to be followed.

We have heard all too often from a long line of DOE managers how serious LANL issues are and changes are needed. However, Mr. Chairman, it is my professional opinion that no one now or previously in the Department has had the commitment, the dedication, and absolute resolve to change the way this department is managed and the way this laboratory is managed than Secretary Bodman and Deputy Secretary Sell. It is imperative that the NNSA and the Los Alamos site office in particular follow the leadership of the Secretary and the Deputy Secretary and must immediately enhance NNSA capabilities to effectively oversee the contractor performance now and in the future.

Mr. Chairman, one other note, in the course of this hearing, there may be privacy issues that arise, and I would like just to recognize that Eric Fygi from General Counsel is here and representing the Department.

[The prepared statement of Mr. Podonsky appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you.

Before we move to our next witness, we should note that Congresswoman Heather Wilson from New Mexico is a member of the full committee, but not on the subcommittee, but we welcome her participation here today. Thank you.

With that, we will next hear from Ms. Danielle Brian, executive director of Project on Government Oversight.

Ms. Brian.

**TESTIMONY OF DANIELLE BRIAN, EXECUTIVE DIRECTOR, PROJECT ON GOVERNMENT OVERSIGHT**

Ms. BRIAN. Thank you for inviting me to testify today.

I am Danielle Brian, executive director of the Project on Government Oversight. We have been investigating and exposing security failures in the nuclear weapons complex since 2001.

Despite the creation of NNSA, security failures have continued to plague the complex, especially at Los Alamos. Now NNSA Administrator Linton Brooks has been asked to resign, and our Nation's secrets have been mishandled by Los Alamos again. Not only have NNSA and U.C. failed to correct security issues, but now there will be even less oversight of Los Alamos as a new pilot program has been implemented at Los Alamos in which oversight has been handed over to the contractor themselves. Perhaps this new legislation that Congressman Barton has introduced could help turn the tide on this disregard for Federal oversight.

Since 2001, there have been at least seven instances in which classified information was mishandled at Los Alamos, and I suspect there were many others that have simply flown below the radar. Classified computer disks have gone missing. Computers that may have contained classified information have somehow disappeared from lab property, either having been stolen or lost. Classified information has been transmitted through unsecured e-mail, and the list goes on.

The cybersecurity episode has occurred on average nearly once a year since POGO began its investigations, and all of these instances occurred after the infamous episode of the two missing hard drives which were later discovered behind the Xerox machine.

Now, in the recent incident, a subcontractor employee freely took over 200 pages of hard-copy, classified documents and over 400 classified documents on flash drives to her home, which she shared with a drug dealer. This could only have happened if there were a complete collapse of multiple supervisory and security systems. It was only by happenstance that she was caught, not because an effective security system was in place. We would never have known about the security breach if it hadn't been for a domestic disturbance.

Furthermore, we have no way of knowing how many other instances like this there are out there that we don't know about. It is important to remember that NNSA attempted to keep this incident secret from Congress and the public until POGO learned about it 8 days after the local police raid.

After the most recent security incident, a cybersecurity audit was launched, and according to a lab e-mail from just a few days ago that I asked to be submitted for the record, quote, "As a result of the preliminary findings of the cybersecurity audit"—this is just a week and a half ago—"LANL has agreed to suspend all non-essential classified, computing activities for at least the next 48 hours by the close of business today."

And this is not the first time security failures have significantly impacted operations at the lab. In 2000, then-Secretary Bill Richardson announced a new system so that there would no longer be classified, removable electronic media to be lost or stolen. The labs essentially ignored the order. In May 2004, then-Secretary Abraham announced that the complex was going to have a new system doing essentially the same thing. Again, the labs essentially ignored the order. I suspect Secretary Bodman will soon be announcing a new initiative to solve cybersecurity problems, and I am sure he is genuine in his beliefs that his directives will fix the problems, but those of us who have been around for a while have reason to be skeptical.

In addition to cybersecurity failures, Los Alamos continues to suffer from a litany of other problems, and while Los Alamos is a big problem, it is by no means the only problem in the nuclear weapons complex as other sites are also currently facing their share of serious problems.

Despite these other sites that urgently need attention, Los Alamos does stick out as the bad child. Why? There is a joke around the complex that goes something like this: The Secretary of Energy tells the three national labs to jump. Sandia asks, how high? Livermore makes an excuse for why it is too busy to jump, and Los Alamos asks who the Secretary of Energy is.

Los Alamos sticks out as the bad child because of its consistent and utter disregard for Federal oversight. At this rate, as was mentioned before, we can all schedule next year's hearing right now given the likelihood we will still be discussing problems at Los Alamos unless the entire incentive system is reversed.

I have enumerated in my written testimony a number of specific recommendations, but in the interest of time, to highlight them, first is that NNSA, or perhaps simply the Department of Energy, needs to make it a priority to fund oversight and promote Federal employees who are thorough in their oversight work. In its current

state, the Los Alamos site office is nonfunctional. There are over 20 vacant Federal positions in that office.

Officials should also be held accountable if they do not implement the recommendations made by the two gentlemen who are sitting at the witness table, the Department of Energy's Inspector General and the Office of Health, Safety, and Security. As we have mentioned before, there are numerous reports that have been issued on these issues, but no one gets in trouble when they don't do anything about what these people have recommended.

The Performance Incentive Fee in the Los Alamos contract should be recalculated and equally weighted to reflect the equal importance of accomplishing the mission with ensuring security and doing so safely. Of the $51 million that is currently on the table for fiscal year 2007 in the performance fee for the Los Alamos budget, only 6 percent, or $3 million of that amount, is tied to security. Fortunately, that small percent is not set in stone and should certainly be revisited and dramatically increased. At the very least, DOE should cut the Performance Incentive Fee for the most security—for the most recent security debacle at Los Alamos.

DOE should also be disallowing costs—this is a cost-reimbursable contract, so they should be disallowing costs with Los Alamos' as failure to perform adequately.

POGO also recommends that the "at will" employment provision at Los Alamos be changed for their employees because currently, if an employee is the bearer of bad news to management, the employee can be fired at will, creating exactly the wrong incentives. This is an important issue for the committee to be conscious of as it is of particular concern for Livermore employees who are not currently operating under this condition, but, as you see, appears to be poised to retain the contract at Livermore. There is, in fact, concern that this will now affect or be affected for the Livermore employees as well.

I am thrilled that the committee has already undertaken our next recommendation to audit the missions currently being conducted at Los Alamos. I think that's a very important effort the committee is undertaking.

In closing, DOE will soon be submitting a request of $150 billion to fund a wildly ambitious project to revamp the nuclear weapons complex known as Complex 2030. Before any funding for further expansion is approved, I respectfully suggest that Congress must have confidence in the mission and in the ability of the complex to carry out that mission safely and securely.

Thank you.

[The prepared statement of Ms. Brian appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you.

We will begin questioning.

Mr. Friedman, your investigation of the recent incident at Los Alamos revealed the lab security framework was seriously flawed.

For example, is it true that a number of key areas, including security policy, was nonexistent, applied inconsistently or not followed?

Mr. FRIEDMAN. That is correct, Mr. Chairman.

Mr. STUPAK. In 2004, the lab was shut down when we did this massive review. Wasn't that one of the recommendations in 2004?

Mr. FRIEDMAN. It was, and actually you could trace it back to 1999, in essence.

Mr. STUPAK. Then what is it? Why are we having such problems with Los Alamos? As Ms. Brian says, Secretary Richardson gave an order, Secretary Abraham, now Secretary Bodman, and we have been reassured by Mr. Podonsky that things are going to change. For instance, in 1999—that's, what, 8 years now—there have been 11, 12 hearings. Any answers?

Mr. FRIEDMAN. Well, I use—I thought the ultimate question would come a little bit later. I didn't expect it on the third question, Mr. Chairman.

Mr. STUPAK. I've only got 8 more years to mess around, but we don't with this lab.

Mr. FRIEDMAN. Of course, it is an issue that we have thought about a great deal. We devote a lot of resources to Los Alamos, and you and I have had this discussion before, obviously.

I think one of the problems that we've found consistently is the question of sustainability, Mr. Chairman, if I can put it that way, use that term. There are a lot of good intentions. People start off with the right set of principles. They have new policies, new procedures that they begin to implement, and the implementation begins, but there is not the stay with it, the closing the deal, the sustainability that is necessary to go from a good idea to implementation, to execution, and to consistency, and I tend to think that's one of the fundamental problems that we have seen at Los Alamos over time. I said there are good starting principles, but no follow-through, a lack of follow-through.

Mr. STUPAK. There is a lack of follow-through because of turnover in personnel, or we lose interest in the principles that we are supposed to put forth?

Mr. FRIEDMAN. I think it's the latter rather than the former. Certainly there is a turnover in personnel, but I don't think—my sense is that is not the heart of the problem.

Mr. STUPAK. Well, in your recently released report on Los Alamos, in doing your work your team uncovered a number of much broader concerns than merely the concerns related to the October incident. Let me read from your report, and I am quoting now.

It says, "Our review revealed a serious breakdown in core laboratory security controls," and your report reached the conclusion, and it states, "In short, your findings raise serious concerns about the laboratory's ability to protect both classified and sensitive information systems."

I presume you still stand by that report and that conclusion?

Mr. FRIEDMAN. Yes. Yes, we do.

Mr. STUPAK. There has been a lot of talk this morning about maybe we should just change the focus of this lab, or some of the missions must be shifted to other labs like Sandia. It is a very, very large complex.

Your thoughts on that suggestion.

Mr. FRIEDMAN. Well, I am not here, Mr. Chairman, as a shill for the laboratory, but as a number of members of the sub committee have identified this morning, it is an extraordinary institution.

Sixty-three percent of the people there or thereabouts have postgraduate degrees. They're eminent scientists. Last year lab personnel won, I believe, five R&D 100 awards. There are 28 E.O. Lawrence Award winners there.

It is an extraordinary institution, and I caution, if I might, that before we do anything truly radical—and I understand the motivation and where it's coming from—that we make sure we balance so that we don't throw out the baby with the bath water, if I can put it that way. So I hope that we give the new contractor—I mean, after all, this took place 2 months ago. When we last spoke, Mr. Stupak, we agreed that the new contractor was coming on board, and they deserved an opportunity to turn the situation around. This series of events occurred within 2 months or 3 months after they took over. They identified a number of preconditions—preexisting conditions that concerned them before they assumed responsibility, and cybersecurity was one of those preconditions.

I am hopeful that we can give them a chance, with increased Federal intervention and oversight, to do what they were hired to do, which was to enhance dramatically the management of the laboratory, including better security and better cybersecurity specifically.

So I understand, at some point down the road, a more dramatic, a more radical departure may be warranted conceivably, but at this point I hope we give them the benefit of the doubt, at least for a period of time, recognizing that the problem that we face here is a very, very serious national security problem.

Mr. STUPAK. Sure, but if it wasn't for the Los Alamos County Police Department, we would not even know about this incident. How many other breaches are out there that we do not know about because there has been no mechanism in place to detect it, or even if it was detected, from your testimony, no one at the lab seems to want to follow up on it?

Mr. FRIEDMAN. I said in my testimony that one of the most frightening parts of this whole incident is that, had it not been for an inadvertent set of circumstances totally unrelated to this issue, we might not have known about it today. We might never have known about it, and that is a frightening thought. And we have identified a couple of suggestions of a more intense activity logging at the laboratory and monitorship with new software that can be costly, but may be necessary to make sure that other breaches, other similar breaches, are not occurring. Prevention is the key, in my view.

Mr. STUPAK. OK. My time is up. Hopefully we will go around for a second round.

Next let me turn to the ranking member, Mr. Whitfield from Kentucky.

Mr. WHITFIELD. Thank you very much, Mr. Chairman, and I thank the witnesses for their testimony this morning.

All three of you have extensive experience in this area, and the consensus appears to be that Los Alamos is sort of, for lack of a better term, the problem child. All of these weapons labs have had some problems, but the Los Alamos problems seem to be more serious and certainly more frequent. And I know that the University of California does manage the Lawrence Livermore—has the con-

tract for that, and for 60-some years had the contract at Los Alamos and now is a 50-percent participant in the new consortium.

That's correct, isn't it?

Mr. FRIEDMAN. That is roughly correct, yes.

Mr. WHITFIELD. OK. Now, just from your personal experience, how would you explain if you were talking to a Rotary Club in Hopkinsville, KY, what your theory is as to why Los Alamos has so many breaches when you have had, for many years, the same management contract responsibility at both Los Alamos and Livermore?

I would like to ask each one of you to just give me your impressions as to why that is the case.

Mr. FRIEDMAN. Well, I don't, Mr. Whitfield, have a good answer for that question. I mean, it is an extremely important question, and despite spending years at looking at all of the laboratories, I don't have a good answer. I wish I did. I think it would get to the heart of the cure.

But what I would say is that Los Alamos is slightly different. I think Livermore—and I might be wrong about this—is essentially located on 1 square mile of territory. Sandia is larger, but I think none of them have the diversity, the geographic diversity, if nothing else, and that may be a contributing factor to the problem. I mean, as we have pointed out in the testimony, and as has been discussed earlier, we found, I believe, 2,700 classified computing environments. We have long taken the position that closing, reducing the footprint is the way to go, and it may well be that the number of classified computing environments, the number of classified materials that are there in sheer numbers, may be part of the problem.

Mr. WHITFIELD. What about you, Mr. Podonsky? What would be your thought.

Mr. PODONSKY. Well, sir, to put it in context, we've been inspecting independently the operations of this lab as well as the entire complex now since 1984, and our observations and continuing issues that have developed is the lack of accountability, which is why I say in my opening testimony and why the committee here all talks about the preceding managers that have come up and make the statements about, now we did it, now we are serious, which is why I made a very poignant statement that I do believe that Secretary Bodman and Deputy Secretary Sell not only are as committed as previously, but they are taking action. I have been through a number of previous Secretaries through all of these incidences and come up with great plans, but they don't get converted into action.

Mr. WHITFIELD. OK.

Mr. PODONSKY. So, specifically to your question, sir, I would say that it's accountability and holding people responsible for the jobs that they have out there, and we have not seen that consistently at Los Alamos through the years and at some other places, but predominantly at Los Alamos.

Mr. WHITFIELD. Can I assume that you and Mr. Sell and Mr. Bodman are supporting the Barton-Dingell-Stupak-Whitfield legislation to remove NNSA from the equation.

Mr. PODONSKY. I can't speak for the Secretary or for the Deputy Secretary. I can only speak for myself, and I have not seen that correspondence.

Mr. WHITFIELD. OK.

Ms. Brian, what about the question?

Ms. BRIAN. I have been struggling with this question for a while myself. I think it is a combination, as I mentioned in the joke that goes around, that there is a different attitude at Los Alamos, and I think because of that different attitude, they are more difficult at the Federal level to manage. And I think the bottom line is when you get the push-back from Los Alamos, and the Federal structure is not there, really, with the willingness to stick with them and demand change, I think that is where there is really the breakdown that I think we can be enforcing on.

Mr. WHITFIELD. OK.

Mr. Podonsky, let me ask a question. In 2004, Los Alamos was closed down for 6 months because of security breaches. What was the dollar amount of the penalty that the University of California system had to pay at that time for that breach?

Mr. PODONSKY. I am not aware of what the penalty was, sir.

Mr. WHITFIELD. Who would know that.

Mr. PODONSKY. I believe the next panel—or the third panel would.

Mr. WHITFIELD. OK.

Mr. BARTON. Would the gentleman yield on that?

Mr. WHITFIELD. Yes, sir.

Mr. BARTON. Was there any penalty?

Mr. PODONSKY. Mr. Barton, I'm not aware of any penalty that was associated with this shutdown.

Mr. BARTON. So there was zero penalty then?

Mr. STUPAK. If the gentleman would yield, it cost the taxpayers $350 million. Who paid for that other than the taxpayers? Are we back with the same problems?

Mr. WHITFIELD. My time has expired.

Mr. STUPAK. I thank the gentleman.

Mr. Dingell, questions? We are doing 5 minutes now, and we'll go another round.

The CHAIRMAN. Mr. Chairman, thank you for the courtesy.

I find this again, as I indicated, sort of a Groundhog Day or perhaps deja vu all over again.

Mr. Podonsky and Mr. Friedman, I would like to summarize some of the key findings of your recent work at Los Alamos.

Mr. Friedman, isn't it correct that your team went out to investigate the event, and that you, in fact, spent a relatively short period of time on the ground, yet in that short period you found a lot of serious problems at the site? Is that correct?

Mr. FRIEDMAN. That's correct, Mr. Chairman.

The CHAIRMAN. Mr. Friedman, in fact, didn't your investigation of the recent incident reveal that in a number of key areas that security plans and policies were either applied inconsistently or not followed in some cases or, in others, nonexistent?

Mr. FRIEDMAN. That is correct.

The CHAIRMAN. Mr. Friedman, isn't it true that your audit revealed that the critical cybersecurity internal controls and safe-

guards were not functioning as intended at various places across the LANL?

Mr. FRIEDMAN. Yes, sir.

The CHAIRMAN. Now, Mr. Friedman, isn't it also correct that monitoring by both the laboratory and Federal officials was also found to be inadequate or, in other cases, nonexistent?

Mr. FRIEDMAN. It was.

The CHAIRMAN. Isn't it correct also, Mr. Friedman, that even though the network engineering officials and others within the lab's Chief of Information Office expressed concerns about open ports and problems with managing tamper-indicating devices, and these concerns were largely ignored by LANL officials?

Mr. FRIEDMAN. Yes. And can I elaborate on my answer on that one, Mr. Chairman?

The CHAIRMAN. Now, Mr. Podonsky, I believe your testimony also says that Los Alamos received the lowest set of performance ratings for security and emergency management since 1999; is that correct?

Mr. PODONSKY. Yes, sir.

The CHAIRMAN. Now, Mr. Friedman and Mr. Podonsky, both of you know that I've been working at this security problem for more than a little while.

Mr. Podonsky, you indicated Los Alamos received some of the lowest scores since 1999 on security issues.

Mr. Friedman, your report found that there was a core breakdown of Los Alamos' ability to protect classified information.

That's correct, is it not, gentlemen?

Mr. FRIEDMAN. Yes.

Mr. PODONSKY. Yes, sir.

The CHAIRMAN. Would you like to tell us what is going on here? And we are going to ask the Secretary why we need to keep on having these hearings.

What comments do you have, gentlemen?

Mr. FRIEDMAN. Well, I think your series of questions, Mr. Chairman, from my perspective, basically outline—as you say, we have been on the ground for a relatively short period of time, although we have a resident staff at Los Alamos who spend a lot of time there, but to say that the system we found in place was inadequate to protect the material is an accurate reflection of what we found.

The CHAIRMAN. Mr. Podonsky, are you going to comment?

Mr. PODONSKY. Yes, sir. I do not disagree with your statements. The only thing I would like to again point out to the committee is that, when our inspection team was at the site, we again did determine that the nuclear material was protected, and that's not insignificant. That is something, Mr. Chairman, as you'll recall back in the 1980's we paid a lot of attention to. That doesn't make it a good story, because the classified matter is something of grave concern to all of us, and as my colleague Mr. Friedman has talked about, we do believe that Los Alamos has a mission to perform for the country, but the security performance that they've demonstrated inspection after inspection continues to leave us concerned and baffled.

The CHAIRMAN. Now, I would like to direct this to the panel, but with particular emphasis to Danielle Brian.

A statement here says this,

Now, in the most recent incident, a subcontractor employee freely took over 200 pages of hard-copy, classified documents and over 400 classified documents on flash drives to her home, which she shared with a drug dealer. This could only have happened if there was a complete collapse of multiple supervisory and security systems. It is only by happenstance that she was caught, not because of an effective security system in place. We never know—we would never have known about this security breach if it hadn't been for a domestic disturbance.

Then she goes on to say this,

Furthermore, we have no way of knowing how many other incidences like this are out there or have flown below the radar. It is important to remember that NNSA attempted to keep this incident secret from Congress and the public until POGO learned about it about—learned about it 8 days after a local police raid.

Then here, as a side note,

If media reports and statements by investigators are accurate, this most recent case points to extraordinary failures in the personnel security clearance process in addition to cybersecurity failures at the lab.

Now, my concern here is we seem to have a situation where the process has broken down, whether there just is a lack of will or there isn't a competence on the part of the agency to do what needs to be done. Would you each like to tell us what your feelings are on this matter?

Could I just ask for 1 minute more, Mr. Chairman, please?

Mr. STUPAK. Without objection.

The CHAIRMAN. What do you have to say, ladies and gentlemen?

Ms. BRIAN. Well, that is what I had to say.

I think the problem here is a combination of extraordinary breakdowns. Maybe the systems aren't even there, and it's not a case of broken systems, but I am also equally concerned that at the time this was becoming known at Los Alamos, there was a real effort to make sure that people in the Congress didn't know about it. They were hoping they would make this go away.

The CHAIRMAN. Thank you.

Mr. Podonsky and Mr. Friedman.

Mr. PODONSKY. We did not investigate the actual circumstances. As I said in my testimony, Mr. Friedman did the investigation. We were there doing a comprehensive safeguard security inspection which gave us an overall, comprehensive review of the various topics, but we did see clearly the laboratory suffering from a lack of policies, procedures, adequate management, adequate oversight—both contractor and Federal—and all of that would contribute, we believe, to the incident that the Inspector General investigated.

The CHAIRMAN. Thank you.

Mr. Friedman.

Mr. FRIEDMAN. Mr. Chairman, you made a point in your earlier questioning that I wanted to comment on which I think would respond to this question as well.

You pointed out, which was a good read of our report if I may say so, that we found that, I think it was in the March 2006 time frame, there was e-mail communication, within the laboratory about the concern about open ports. So, in other words, the institution itself identified that as a problem, and there was a fair amount of traffic, e-mail traffic, on that issue.

And it gets to the point that I was trying to make earlier about closing the deal, sustainability and the ultimate fix, and that is that, tragically, even though it was discussed extensively—and I think it was in March 2006, and I don't have that instant recall. I think that's the right date—no one took it to the next step, which is to make sure that the proper fix was implemented to address the concern. Now, it was not of universal concern. There were people at the laboratory who didn't think the open ports were a serious problem, but there were enough people who did, and it would seem to me—and I think this is, perhaps, revealing as to the essence of the problem—that they didn't address the problem then and resolve it.

The CHAIRMAN. Your comments earlier in response to a question were that we ought to give the laboratory the benefit of the doubt. I wonder if, after this commentary, you are in agreement that we ought to give them the benefit of the doubt.

Mr. FRIEDMAN. Well, I think I'm the one who said it, Mr. Chairman, so I will stand by the statement.

First of all, I think the laboratory is an extraordinary institution, and second, I think that in fairness—and believe me, I am not here—I probably write more critical reports about Los Alamos than anyone, but in fairness, I think the new contractor is really brand new, was brand new when this occurred, and they deserve an opportunity to try to fix the problem, and if they can't fix the problem, I'd be the first one to sit before you and tell you that a much more radical solution needs to be tried.

The CHAIRMAN. Thank you, Mr. Chairman.

Mr. STUPAK. Next, Mr. Barton from Texas.

Mr. BARTON. Thank you. Some of the statements just kind of strain credulity.

Mr. Friedman, who was the old contractor?

Mr. FRIEDMAN. The University of California.

Mr. BARTON. Who is the new contractor?

Mr. FRIEDMAN. I think it's a consortium. I believe it's a limited——

Mr. BARTON. Come on. Who is the new contractor? It is the University of California. They've got a consortium, and there may be some different players, but the University of California has had this contract for 60 years. They were the old contractor; they are the new contractor; is that not correct?

Mr. FRIEDMAN. Well, I——

Mr. BARTON. Yes or no?

Mr. FRIEDMAN. No, actually.

Mr. BARTON. It's not?

Mr. FRIEDMAN. No.

Mr. BARTON. They are not part of it?

Mr. FRIEDMAN. They are the primary science player, there is no question about that, but the whole concept, as I understand it——

Mr. BARTON. They have 50 percent of the contract.

Mr. FRIEDMAN. That's true, but it——

Mr. BARTON. The person who has been moved to the new—who is the new lab director is a University of California employee.

Mr. FRIEDMAN. That is correct.

Mr. BARTON. The Bechtel individual, who is the top person, has already left; is that correct?

Mr. FRIEDMAN. That is correct, yes.

Mr. BARTON. Now at least be honest with the committee.

Mr. FRIEDMAN. Well, I have tried to be honest, Mr. Chairman.

Mr. BARTON. This semantics about old and new is an affront at least to me. My gosh. Is it not true that under the new contract the performance part of it is at risk if there is a security lapse?

Mr. FRIEDMAN. Well, let me give you the read of the contract as I understand it, Mr. Barton, and there are people at least on the third panel who are the negotiators of the contract who can give you more detail.

In its full bloom, my understanding is there's about a $70 million-a-year potential award fee, 30 percent of which, as I understand it, is——

Mr. BARTON. It is $73,280,000 to be exact.

Mr. FRIEDMAN. As I understand it, 30 percent of it is fixed, and 70 percent is at risk. That's the way I understand the formulation of the contract. I believe there also is a provision—and I'm not an expert on the contract. There are people here who are. I believe there are provisions that, in extraordinary circumstances, at least the entire at-risk portion can be withheld from the contract.

Mr. BARTON. Is it not true that, in your testimony, you suggested that there'd be a serious withholding of the incentive part of the contract?

Mr. FRIEDMAN. Yes, sir, I did.

Mr. BARTON. Do you want to put a number on that? How serious is "serious"? The safeguard and security execution part of the mission success is $3 million.

Mr. FRIEDMAN. Yes.

Mr. BARTON. Is that serious, or do you think "serious" would be $10 million?

Mr. FRIEDMAN. No, I think it may be $3.8 million, Mr. Chairman, but I don't think that's serious money.

Mr. BARTON. Mr. Stupak is the chairman. I am the ranking member.

Mr. FRIEDMAN. Mr. Ranking Member then. I apologize.

Mr. BARTON. I'm just at a loss here.

I'm going to ask Mr. Podonsky something.

The gentle lady next to you indicated that the contractor at the site office has 20 vacancies. Is that your understanding?

Mr. PODONSKY. I do not know the exact number, but, yes, I do know that they are short.

Mr. BARTON. What is the number—what would be the full complement? Is it like 40 people at the site office, 100 people?

Mr. PODONSKY. Mr. Barton, I do not have that number. That would be—the NNSA would have that number, but I would just tell you that I do know that they're short on qualified Federal staff.

Mr. BARTON. OK.

Ms. Brian, do you know how many people would be the full complement if they were fully manned at the site office?

Ms. BRIAN. I don't know. I do know that of the 20 vacancies, a large percentage of them are in the security and safety area for the site office.

Mr. BARTON. Does that, to you, indicate that the Department is serious and the new contractor is serious about this?

Ms. BRIAN. Well, that's actually the Federal Government.

Mr. BARTON. I understand that.

Ms. BRIAN. So my worry is that DOE isn't serious or NNSA.

Mr. BARTON. OK. Could we get that information, what the total staffing is and what these vacancies are?

Mr. Podonsky, do you think that we ought to fill those slots?

Mr. PODONSKY. Yes, sir. I think that they need to be filled with the right qualified people because this laboratory needs appropriate Federal oversight from the NNSA.

Mr. BARTON. My time has expired, Mr. Stupak.

Mr. STUPAK. I thank the gentleman.

Ms. DeGette.

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

Mr. Friedman, I wanted to ask you some questions about what you had said in response to several of the other Members' questions.

The first thing is you said that we really need to give this new contractor a chance, and that we need to—if we need to do something dramatic, we should do it down the road. So I'm kind of wondering how long is that road, because I've been sitting here in this subcommittee since 1999 hearing these assurances. I understand what you're saying about the quality of people that we have there and the high-level work that's going on, but how much longer do you think we need to be patient? How much longer do we need to give these folks to fix these problems?

Mr. FRIEDMAN. Well, my view is, from the start date, it should be probably 1 year.

Ms. DEGETTE. One year from June? So until this June?

Mr. FRIEDMAN. This June, yes.

Ms. DEGETTE. And do you think that—and my second question is how will we know if the new contractors have fixed the problem? Will we know that if the local law enforcement authorities bust some people or if the local newspapers have an expose? How are we going to know if the problem's been fixed?

Mr. FRIEDMAN. Well, with 12,000 people there, you may never know for sure. I understand that, but I think in the next 6 months' time what will be devoted by the Department is an intensive examination of all aspects of the function of the lab to make sure that the problems have been addressed.

Ms. DEGETTE. Well, do you think we haven't had that intensive examination in the many past times that we've worked on this?

Mr. FRIEDMAN. I do not think we've had that intensive examination.

Ms. DEGETTE. That's just appalling to me because they closed down the lab after we visited in 2004, and you don't think they did that intensive examination?

Mr. FRIEDMAN. Well, I think they did an intensive examination, but the point I've been trying to make is that, once they did the intensive examination, did they sustain an aggressive program to address the problems that were identified, and that's the concern that I'm expressing today.

Ms. DEGETTE. Do you have some specific recommendations as to what the Department can do to do this intensive examination within the next 6 months?

Mr. FRIEDMAN. Yes.

Ms. DEGETTE. Would you mind supplementing your responses by delineating those specific things that the Department can do?

Mr. FRIEDMAN. Certainly.

Ms. DEGETTE. Thank you.

Ms. Brian, what is your view about all of this that we should give some time for the Department to clean this up, and then it'll be fixed?

Ms. BRIAN. I respectfully disagree with Mr. Friedman.

I think that the first thing is that the DOE needs to get its house in order and NNSA, and then I think the contractor will ultimately follow in line. I just think that the Government hasn't been doing its end of the job.

Ms. DEGETTE. And what do you think the Government can do?

Ms. BRIAN. I think we need to have sincere—well, one of the things that I think is really important is that a lot of these issues, as I discussed in my written testimony, are infuriatingly familiar.

Ms. DEGETTE. Right.

Ms. BRIAN. We've known about these problems before. We've had IG and various iterations of Mr. Podonsky's office make recommendations, and nothing has—no one has required the people at NNSA to actually implement these recommendations. We've had Secretaries—in fact, the issues that—I think it was Mr. Walden who was raising them with the glue sticks. Those were the kinds of things that were supposed to have been dealt with back with Secretary Richardson——

Ms. DEGETTE. Right.

Ms. BRIAN [continuing]. And they've been buying new computers for the last 10 years with the USB ports because, as I learned, the people who were in charge of buying the computers at Los Alamos weren't really talking to the cybersecurity people to realize that they didn't want to have computers with USB ports.

Ms. DEGETTE. Mr. Podonsky, do you have a view on that? Do you think this problem can be fixed in 6 months without any substantial changes?

Mr. PODONSKY. No. We do believe that there needs to be substantial changes, and we do believe that this Secretary and the Deputy Secretary are moving towards that direction. They're not just promissory notes of the past. We've seen actions taken that we have never seen in 25 years of this Department where people were actually held accountable.

You do need to have performance measures that the contractor's held accountable against. We also have an enforcement function within the office that we also need to employ.

So there are a lot of—a lot of tools for the Department to exercise now and get on with fixing the laboratory together with fixing the NNSA and the policy of the Department.

Ms. DEGETTE. Do you think, Mr. Friedman, that the physical size of Los Alamos is a problem?

Mr. FRIEDMAN. Yes, I think it's a challenge.

Ms. DEGETTE. And what can we do to deal with that challenge, do you think?

Mr. FRIEDMAN. Well, first of all, we can make a concerted effort to consolidate functions, reduce the number of vaults, reduce the number of classified computing environments. I don't know how practical that is. I think it's something that we need to look at very carefully.

Ms. DEGETTE. Thank you.

Mr. FRIEDMAN. Second, I think we need to enclose the footprint so that the security perimeter is reduced so physical security will be—will be somewhat easier.

Ms. DEGETTE. Mr. Chairman, I think a good time for a follow-up hearing—I mean, we should have some interim ones, but we also need to have one in June to mark the 1-year anniversary and see how they fixed all these problems.

Mr. STUPAK. Mr. Burgess, questions?

Mr. BURGESS. Thank you, Mr. Chairman.

Mr. Podonsky, we have been through—I have been through at least 2 years of these travails, and it seems like every security incident that has been reviewed has been by an employee who has received a security clearance; is that correct?

Mr. PODONSKY. My recollection is that predominantly cleared individuals have been violating DOE's requirements.

Mr. BURGESS. Was that the case in this most recent event in October?

Mr. PODONSKY. I believe so.

Mr. BURGESS. OK. And the individual who claimed assault at the bar a couple of years ago, was that also an individual who had been cleared?

Mr. PODONSKY. I believe that is the case.

Mr. BURGESS. Is there a problem with how we're granting clearances to—how NNSA is granting security clearances?

Mr. PODONSKY. The personnel security process is one of—the task force that the Secretary initiated at the beginning of this event after Mr. Friedman's report was to look at personnel security, specifically at the case in question as well as DOE-wide. Concurrently there was a review that had begun by Deputy Secretary Sell in May of last year where we were looking at personnel security processes.

So the short answer is, yes, we do believe that personnel security processes within the Department and, in fact, the entire executive branch which are being looked at by the OMB right now are something that we need to get on with, and that's what we're doing, and we're going to be making recommendations to the Secretary and the Deputy Secretary at the end of February of what to do with the personnel security program within the Department of Energy.

Mr. BURGESS. Will that include any type of program that looks at cleared individuals in an ongoing fashion?

When I was there in July 2005, it was right after the credit card abuses came to light, and it appeared, as I recall, that those were cleared individuals who had then subsequently developed either domestic problems or substance abuse problems that led them to misuse the credit cards, and you can just imagine that other things may have happened also as a result.

So will there be an ongoing evaluation?

Mr. PODONSKY. The recommendations that, I believe, are coming out of the task force will be covering both from the beginning of hiring all the way through current employees so that we have an ongoing review of people holding clearances.

Mr. BURGESS. Inspector Friedman, do you think, in retrospect—I reference the RFP process that the lab just went through. Chairman Barton also referenced the contractor. Do you think that was an open and fair process?

Mr. FRIEDMAN. Frankly, Dr. Burgess, I have no information that it was not. Unfortunately, there were two proposals, as I understand it, in the final field, but I have no reason to believe it was not open and fair. I have no information to that effect.

Mr. BURGESS. Would that be in the purview of the Inspector General's Office to know that, or is that outside your capabilities?

Mr. FRIEDMAN. No, it's not outside our capabilities, and, by the way, if there had been concerns by proposers that were not considered, it would not be unusual for us to get complaints about that, and to the best of my recollection, and I could be wrong about this, I don't think we received any complaints along those lines.

Mr. BURGESS. And yet some of just the traffic from the bloggers on line—and I realize that that carries its own inherent dangers, but there is some question as to whether or not the current contractor was, in fact, the best one and is the best one going forward.

Again, I don't know whether it's the purview of this committee to investigate that process, but, Mr. Chairman, I for one certainly wonder if we oughtn't to look at that.

Ranking Member Barton asked about the fines. The amount of money levied so far against the current contractor, do we have a dollar figure on that?

Mr. FRIEDMAN. Are you referring that question to me?

Mr. BURGESS. Yes, sir.

Mr. FRIEDMAN. I do not have a number on that, no.

Mr. BURGESS. Is there a way to—for anyone, is there a way to get that dollar figure on the fines levied against the contractor?

Mr. FRIEDMAN. Well, respectfully, the third panel, I think, includes people who would have that information.

Mr. BURGESS. Does the contractor recognize the amount of dollars that they are putting at risk?

Mr. FRIEDMAN. I suspect they know the contract intimately.

Mr. BURGESS. OK.

Mr. Friedman, just to finish up, your statement said the criminal investigation into the matter last fall is ongoing and may yet reveal additional security problems.

In an open session can you expand on that statement?

Mr. FRIEDMAN. Well, simply, the FBI has been conducting a criminal investigation from the get-go, and the purpose of that statement in my testimony—and I think it's in our report as well if I'm not mistaken—is that until their investigation is complete, we don't know what will turn up. There may be more.

Mr. BURGESS. What would be a reasonable time frame for this committee to expect that that investigation will take?

Mr. FRIEDMAN. That's within the purview of the FBI, sir, and I have no idea.

Mr. BURGESS. Mr. Chairman, will we be privy to that report when the Department of Justice completes that?

Mr. STUPAK. That's a good question. We'll double check on it. I don't see why not, but let's double check first.

Mr. BURGESS. All right. My time has expired.

Mr. STUPAK. The gentleman from Louisiana Mr. Melancon.

Mr. MELANCON. Thank you, Mr. Chairman.

I guess, Mr. Friedman, one of the first things when you look at—and I understand there's a problem with the drug use, apparently, with this one particular breach, but apparently there's some additional problems out there within.

Does the staff or the security people require or do the random drug sampling, the urine test, at all on the employees, or is it "you're hired"?

Mr. FRIEDMAN. I'm in open session. Part of your question I think I can address, but part of it I would prefer not to address.

My understanding is—and, again, there are people who are on the third panel who can address the issue of the current policy. My understanding is that they have implemented a random drug test for all Los Alamos employees, but I may be wrong about that, and you'll need to ask the third panel, sir.

Mr. MELANCON. And have you just done that just recently?

Mr. FRIEDMAN. Fairly recently, yes.

Mr. MELANCON. With the time that's transpired with the issue of security breaches and you've replaced the chain of command, the latest chain of command replacement took place when, how long ago?

Mr. FRIEDMAN. June 1.

Mr. MELANCON. June 1 of last year?

Mr. FRIEDMAN. Correct.

Mr. MELANCON. And that was subsequent of the close-down for 7 months in 2004?

Mr. FRIEDMAN. Well, the contract changed hands on or about June 1, 2006, and, yes, it was subsequent to the 2004 shutdown.

Mr. MELANCON. OK. So somewhere between 2004 and last year, which was 2006, how was the lab run? Who was in charge?

Mr. FRIEDMAN. The University of California was the prime contractor.

Mr. MELANCON. And the on-site security?

Mr. FRIEDMAN. They ultimately were responsible for the on-site security.

Mr. MELANCON. Who did they subcontract out for the security? I don't think the University of California is a security company.

Mr. FRIEDMAN. Well, they are at some locations, interestingly enough, and I forget the name of the contractor, to be honest with you; the subcontractor, I should say.

Mr. MELANCON. The diversity of the science—and this is, of course, somewhat new to me—that's out there or the regimens that you have out there of the different scientists, is there some way—and I think maybe you spoke to it earlier. Is there some way to isolate these and provide better security on each sector rather than just have these—and I haven't been to the facility—12,000 people just coming and going wherever they want to go?

Mr. FRIEDMAN. Well, there are a number of secure areas at the facility, and it's worthwhile going to see it. It's quite impressive. So I wouldn't say there are 12,000 people running back and forth at will. It's much more systematic and controlled than that. I'm not sure if there's a practical way of doing it by discipline, but I haven't thought that through, I can't give you a good answer.

Mr. MELANCON. Yes, I'd like to go and see it. The only view I've had of it was from across the valley at a friend's house at night with the lights, so getting in there and looking at it, I guess, close-hand would do me a whole lot of good.

I listened to the frustration of Ranking Member Barton and Chairman Stupak and others who have been here and gone through this for a period of time, and I guess to—we're to June.

Why did it take so long from the 7-month shutdown—and that's another year, year and a half—before we got the new contract in, and now we're waiting a year to see if we're going to get—what's the problems with moving this thing quicker? I mean, I know the numbers are big, but——

Mr. FRIEDMAN. Well, yes. I'm not sure I can give you the precise timeline, but in the general sense, the recompetition of this contract was a very turbulent issue. It was a very costly issue. It was a very labor-intensive issue, and it was a time—a time issue as well. It takes a long time to prepare the RFP, to address, hopefully, the issues that have been resident at Los Alamos for 64 years, and to go to the street, give people time to propose, to evaluate the proposals, and to move forward.

So I don't know if that answers your question, but it is a very time-consuming task.

Mr. MELANCON. I'm from south Louisiana. I've seen inside baseball, and they're getting plagued down in recovery efforts, so I think I can understand some of it.

Thank you. I have no more questions.

Mr. STUPAK. Mr. Murphy.

Mr. MURPHY. Thank you, Mr. Chairman.

Mr. Friedman, do we have information yet on what was the motive for this theft?

Mr. FRIEDMAN. Mr. Murphy, It would be inappropriate—first of all, I don't know the answer to the question. It perhaps resides with the FBI, but at this point I don't know.

Mr. MURPHY. Do we know yet—and I guess I would open this to all of you—what, if anything, was—I know there was also talk about printers being bought and things like that—about to what extent things were copied, distributed and sold or who these documents also went to?

Mr. FRIEDMAN. If you're directing that to me, I'll give you the same answer. The FBI really, ultimately, will have to address that.

Mr. MURPHY. The same with Mr. Podonsky and Ms. Brian. Does anybody know yet?

Mr. PODONSKY. I would say the same thing as Mr. Friedman. We don't have the answers to that.

Ms. BRIAN. I can speak to the press reports from her attorney, which were that she was taking the work home to get extra work done, that she was behind.

Mr. MURPHY. OK. Has anybody determined if there has been—if any of these contents have appeared anywhere else besides just there?

I guess what I'm getting to here is, with regard to this information, that even though we're waiting for further details from the FBI, have we learned anything from this yet that can be used to take other steps other than just blocking some of the ways you can put in a thumb drive or something; but have we learned how it affects security, of how it will affect hardware and software inspections, how people come on and off the site, their security clearances? Have we learned things from this, unique to this, that has affected what we're doing overall and what's been implemented, or are we still going to wait for the FBI reports on this?

Mr. PODONSKY. I would start, first of all, Congressman, with a task force that we are heading up on the personnel security piece. We believe there is going to be a lot of serious lessons learned that are going to come out of the specifics to the case as well as the broader issue on personnel security that one of the members of the committee asked earlier.

We believe that, in terms of cybersecurity as well, there are also lessons learned that we know that the CIOs for both NNSA as well as the Department are looking at, and we also know that the third panel will—has, in fact, done a damage assessment that they could probably talk about in executive session.

Mr. MURPHY. And I will look forward to that part.

I was just wondering here, while we're still in a public hearing, what we can assure the American public with regard to some lessons learned, because it concerns me that this subcommittee has looked at these issues for a long time. Your inspections give us pretty solid, yet frightening information on the levels of breach of security, and we're still awaiting another review before we determine what else we need to do when so much has been out there for a while, and so it's just something I just have to continue to raise the question of. What more do we need to know before we really put the heel down on this?

Ms. BRIAN. Congressman, if I could answer one question, I'm hoping by the end of this hearing that one thing that could change is NNSA's pilot program at Los Alamos, which is essentially self-policing for safety and cybersecurity. I'm generally not a big fan of self-policing as a rule, and I think that a facility like Los Alamos hasn't earned the trust of the Congress or the public to be essentially left up to themselves to report when they have problems, and I think that's something that should be changed immediately.

Mr. MURPHY. Anybody else on that issue?

Mr. Friedman, do you have something on that?

Mr. FRIEDMAN. I did want to point out to you, Mr. Murphy, that our report—and I think we have 14 recommendations for corrective actions. They're not all-encompassing, all-inclusive, but we think it's a good start. The Secretary, as I indicated in my testimony, has a task force looking at those, and we'll be interested to see what their report says in February in terms of how to convert those ideas into reality at the laboratory, both at the Federal level and the contractor level.

Mr. MURPHY. Mr. Podonsky.

Mr. PODONSKY. As the independent overseer for the Secretary and the Deputy Secretary, I would just tell you that I have a prejudicial answer, and that is we don't think that self-assessment, by itself, is good, and the contractor should have Federal oversight. That's why we have contractors and the Feds managing them or should be managing them. So, while the NNSA has this pilot proposed, we don't think it's ready for prime time as exemplified by their performance to date.

Mr. MURPHY. And I would add to that. We're waiting for further investigations. We're reviewing these 14 recommendations. It seems to me a lot of time is ticking by, and I'm just frightened, and I shudder to think what is out there and what else could be happening while all these breaches have occurred and continue to occur. So we will hopefully speed up this whole process.

Thank you, Mr. Chairman.

Mr. STUPAK. I thank the gentleman.

Mr. Green from Texas, questions?

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Podonsky, you state in your testimony that 25,000 unclassified workstations and servers were not certified or accredited. What does that actually mean? Are they unprotected workstations?

Mr. PODONSKY. No, sir. I should—I should clarify that the certification and accreditation process makes sure that security features are in place and operating as designed. When you didn't—when they didn't do the accreditation of the 25,000 unclassified workstations, they did do a network accreditation. Our cyber experts tell me that that's not sufficient, because you don't know if you have individual vulnerabilities on those 25,000 computer workstations. So that's something that—what we believe should be done and should be included in their certification and accreditation process.

Mr. GREEN. It seems like—and, again, you've heard it from every Member up here for the last at least 8 years, I guess—we've identified problems time and time again and identified solutions, but for some reason there's no follow-through on closing the deal. I know it's a great task to do—to just deal with those 25,000 workstations and servers, but why wasn't that done before this particular person walked out with the disk? It seemed like that would have come up in the last 8 years before, at least before this committee, and is there a problem, and nobody knows how to implement the solutions to it?

Mr. PODONSKY. Well, sir, we've identified that the lab has inadequate cyber plans, policies and procedures; incomplete risk management processes; weak self-assessment. So there's a whole litany of things that the laboratory could do to fix this.

Mr. GREEN. OK. I imagine this is not news to anyone sitting on this panel for the last 8 years. As I said, I just came back after 6 years off of it.

Why can't it be fixed? Why can't we have this? Since it's a new contract, I assume when it went out for bids, this new contractor was security-conscious, and is it just not an issue that makes it to the floor of the actual Los Alamos?

Mr. PODONSKY. Sir, if you're addressing that to me, I would answer it can be fixed, and I believe, under the current leadership of

the Department, it will be fixed. As I said for my third time now, having listened to all the plans before, to answer your question specifically, it is that the contractors in years past have not been held accountable to do what the Department has expected them to do.

Mr. GREEN. Mr. Friedman, do you have a comment on that?

Mr. FRIEDMAN. Well, a number of failures that we identified in our report, Mr. Green, are low-hanging fruit: plug the holes where they should be, the ports where they should be plugged, essentially segregate duties where they need to be segregated, ensure that there's adequate monitoring. I mean, these are not high-tech, costly, time-consuming, difficult things to do, and they should be done—they should have been done instantaneously, and if the lab has not taken steps to do those at this point, I would be very discouraged and very disappointed.

Mr. GREEN. Well, Mr. Chairman, it seems like I'm refreshing my memory on this. I remember, over the years, we've had—this is really a college campus. The security is mostly research, what they're doing, and they're more interested in that. And it seems like, since the last time I was on the committee, we haven't seen any changes even though it went out for bid, and I hope the next panel, even in closed session, will show us what can be done from—to make sure that this oversight investigation committee doesn't continue to be dealing with what's happening at Los Alamos for almost a decade now, so—and I yield back my time.

Mr. STUPAK. I thank the gentleman.

The Members have just a couple of quick follow-ups. We're going to switch to 2 minutes and just a quick follow-up with this panel, and then we're going to ask Mr. Friedman and Mr. Podonsky to stay because we will go to executive session a little bit later, but we'd like to get the other panels done before we move to executive session.

So, with that, for 2 minutes, I'll just recognize myself for 2 minutes.

In questions Mr. Green put forth and throughout the testimony today, we've heard that the system breaks down; there's broken systems; it's inadequate.

In July 2004, the lab was shut down. They were doing this extensive review. Everything was supposed to be fixed up for that. It cost the taxpayers $350 million.

So what happened? The $350 million and the 6-month shutdown didn't accomplish anything? The systems weren't updated? The holes weren't plugged? What happened? What did we get for $350 million besides a shut-down lab for 6 months?

Mr. FRIEDMAN. Are you directing that to me?

Mr. STUPAK. Sure, Mr. Friedman.

Mr. FRIEDMAN. Look, Mr. Chairman, if I gave anybody the impression by my earlier testimony that I think that the situation you find now is OK and it will get better automatically, I left the wrong impression, and I apologize for that.

I am extremely discouraged and disappointed that after the litany of reports and the series of unsettling events that have taken place, that the simple fixes that are obviously readily available

have not been in place, regardless of whether there is a new contractor or not.

So if you are asking what we got for our own money, it seems to me if this is the result, we did not get a lot for our money.

Mr. STUPAK. As I stated earlier, Mr. Friedman, in your report you said. Reviewing serious breakdown in the core laboratory security controls. Core. Their very basic, fundamental security is broken down. If we couldn't fix it after shutting it down for 6 months and $350 million, how do we fix it now other than we have a new person coming on board?

Mr. FRIEDMAN. Well, I think I tried to lay it out. As I said, we have 14 recommendations in our report, and I try to lay out some bigger-picture items that we talked about. One is the question of real accountability, significant material impact on award fees, reassignments, terminations; perhaps a change of the mix of the mission of the lab is a possibility. So I think there needs to be some really fundamental changes to shake up the system to ensure that there is a sincere dedication to fixing these problems. We haven't seen it yet.

Mr. STUPAK. My time has expired. Let me ask one question if I may.

Los Alamos has a great record. They have great people there, top scientists, some of our best, most sensitive work there, no doubt about that. But I asked a question last hearing and never really got an answer. Maybe you can answer it now after some time reflecting upon it.

What do we do at Los Alamos that cannot be duplicated or done at the other labs? Is there anything so unique that can only be done at Los Alamos and not at the other labs?

Mr. FRIEDMAN. Well, let me try to answer it this way. You did ask that question in a hearing that I participated.

Mr. STUPAK. And no one has come can up with a unique mission.

Mr. FRIEDMAN. It seems to me once you get past the facilities, the physical plant, and there are unique aspects of the physical plant that would cost hundreds of millions, if perhaps billions, to replicate, once you get past the core of the extraordinary intellectual invigoration that exists there, the people with the unique talents, it seems to that—the fundamental issues that go on there could be done someplace else. I think the answer to your question is yes.

Mr. STUPAK. Mr. Whitfield.

Mr. WHITFIELD. Thank you, Mr. Stupak.

Mr. Podonsky, under the terms of the new contract with LANS at Los Alamos, and when it comes time to assess penalties or fees which we had discussed a number of times today, does the National Nuclear Security Administration have the primary responsibility of enforcing the contract?

Mr. PODONSKY. For enforcing the contract, yes, sir.

Mr. WHITFIELD. And could you just briefly explain the process that would be entailed in assessing a penalty under the contract?

Mr. PODONSKY. Not under the contract. I would have to request that you defer that to the third panel.

Mr. WHITFIELD. So you are not involved in that at all?

Mr. PODONSKY. Not in that type of enforcement.

Mr. WHITFIELD. Thank you.

Mr. STUPAK. Mr. Melancon, any questions to follow?

Seeing no other Members present, we will dismiss this panel.

Mr. Friedman and Mr. Podonsky, we would ask you to stay.

Ms. Brian, thank you.

Mr. STUPAK. Our next panel, if we may, would consist of the Honorable Clay Sell, Deputy Secretary of the Department of Energy.

Mr. Sell, again, I have to ask you to since we take all testimony under oath, and did you bring a legal counsel with you?

Mr. SELL. I would just note, Mr. Chairman, the presence of our Deputy General Counsel from the Department of Energy.

Mr. STUPAK. Very good.

OK, sir, I would ask you to please raise your right hand.

[Witness sworn.]

Mr. STUPAK. The record should reflect the witness has affirmatively stated that his testimony would be under oath.

Mr. Deputy Secretary, please, if you want to give an opening statement.

**TESTIMONY OF HON. CLAY SELL, DEPUTY SECRETARY, U.S. DEPARTMENT OF ENERGY**

Mr. SELL. Chairman Stupak, Congressman Whitfield, members of the subcommittee, I welcome this opportunity to appear before you today to discuss security within the Department of Energy and the recent security incident at Los Alamos National Lab.

The national security responsibilities entrusted to Los Alamos are our Nation's most important. The successes that have sprung forth from this great lab in years past and today are properly a source of great pride and great power in our country. The capabilities of the men and women of Los Alamos continue today to make this lab the only place to go for many national security requirements. And, of course, the secrets entrusted to this lab are among the Nation's most sensitive.

These are among the reasons that the facts of the most recent security incident at Los Alamos are so troubling and the source of such tremendous frustration and concern to the Secretary, to me and to many others throughout the DOE enterprise.

And now, despite years of focused attention and the expenditure of millions of dollars, we are confronted again with the security failure, the facts of which suggest we still have a much larger and a much deeper problem.

As has been alluded to, many well-intentioned leaders have worked to improve security at Los Alamos over the last few years, and in many key areas the Department has made substantial progress. But Secretary Bodman and I are less interested in effort, process and good intentions and more interested in results. The results on matters of security at Los Alamos National Laboratory remain unacceptable.

You have already heard from earlier witnesses; in fact, you each have made statements about what have led to the problems and what happened in this recent matter.

Later today you will hear from the Acting Administrator of the NNSA, our Department's Chief Information Officer and the Direc-

tor of Los Alamos National Laboratory in more detail. Therefore, I intend to focus the balance of my remarks on what the Secretary and I are doing to fix the problems and move forward.

First, in the immediate aftermath of learning about the security breach at Los Alamos, we acted immediately to assess the situation and understand the facts. The NNSA Administrator dispatched the Chief of Defense Nuclear Security and the Cybersecurity Team to the site to begin an immediate review of the incident. On October 26, the Secretary ordered the Inspector General to investigate. And on October 30, I personally traveled to the lab to meet directly with those on the ground and to gain firsthand knowledge of the incident and remedial actions to address the problems.

Second, we took quick action to address realized vulnerabilities. On November 8, I issued a memorandum to improve cybersecurity protection for classified computer systems throughout the DOE complex. That memo included immediate direction to every lab and every facility operating a classified system to conduct an examination of the adequacy of its practices and procedures to ensure that classified information is protected using multiple layers of cybersecurity protection including protection against potential insider threats. Also, the memo required an accounting by each lab and facility throughout our complex for full implementation by January 15 of this year. Today I am informed that the entire complex is in compliance. The line managers will be responsible for ensuring continued adherence to this policy.

Third, in response to findings contained within the Inspector General's report issued on November 27, the Secretary directed two specific actions: first the creation of a senior-level ad hoc committee to review all of the recommendations in the IG's report except those concerning the Department's security clearance process; second, the establishment of a task force to review the personnel security programs throughout the entire DOE complex.

Both reviews will conclude and provide recommendations to the Secretary no later than February 28 of this year. Once we have reviewed the results of the laboratory's actions, corporate and Federal validation activities, the Secretary's two task force recommendations and other actions that have been directed, we will follow up—we will follow up and develop additional improvements and additional reviews as necessary.

We will be pleased to discuss with the subcommittee the additional actions the Secretary decides to take once he has received and reviewed the task force recommendations.

Fourth, during numerous occasions, meetings and conversations with the NNSA, with the NNSA Administrator and his team, with the Los Alamos Director, and with members of the Executive Board, the new contractor at Los Alamos, the Secretary and I have expressed our depth of concern, our sense of urgency and clear expectations for accountability from the top of the Department to the bottom of the laboratory, and that these continuing security problems must be addressed, rectified, and prevented in the future.

Fifth, even before the recent incident at Los Alamos, the Department had substantially increased focus and attention to matters of cybersecurity including hiring of a new Chief Information Officer in November 2005 to reinvigorate and strengthen our efforts. Among

other things, he accelerated our efforts to update our cybersecurity order and National Security Systems Control Manual, and has taken numerous actions to improve our Department's cybersecurity posture. We also brought in a new Chief of Counterintelligence and reorganized the office to improve its performance.

Sixth, the Department also previously recognized—and I would add with strong urging from the Congress—that the leadership of the laboratory could be strengthened by competing the M&O contract. And last June a new corporate leadership team took over management of the laboratory for the first time in its 64-year history.

Seventh and finally, because it is our view that we are—that we, the Department, the Secretary and I, are accountable to the President, the Congress, and the American people not just for efforts, but for results, the Secretary and I made the extremely difficult decision to replace the Administrator of the NNSA and bring in new leadership.

Now, only time will tell if we are to be successful, if we are to distinguish ourselves from our predecessors. But the Secretary and I are committed to making the tough decisions required to lead our Department to a level of security performance befitting the great missions the country has asked us to carry out. We have made progress in improving the security across the Department and at Los Alamos, but as the latest incident indicates, we have much more work to do. We remain committed to the task.

I am happy to answer your questions at this time.

[The prepared statement of Mr. Sell appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you, Mr. Secretary.

You indicated that only time will tell whether or not we are going to be successful, and I say this politely, but one of the problems, I think there is a turnover we see at the lab and administration and things like that. Secretary Bodman, with an upcoming Presidential election, will only be there 2 years. Those problems that we see, the problems, the constant problems we see, won't be resolved in 2 years, will they?

Mr. SELL. The efforts to resolve these problems, in my judgment, take continuous effort over the course of the next 2 years and in the years thereafter. Threats evolve, technologies evolve, and require constant vigilance.

Mr. STUPAK. Wouldn't it be easy for folks in Los Alamos to say, well, there is that directive; we have seen that directive for 2 years. A new set of people come in, and we can sit back?

Mr. SELL. Mr. Chairman, that is certainly a limitation of the manner in which the executive branch of our Government operates. I will be gone in 2 years as will the senior leadership of this Department, as will the President, so we are taking great effort to institutionalize the changes that we are making, and I will give you an example.

After a previous incident in 1999, then-Secretary Richardson issued a substantial press release announcing a number of changes to correct the then-perceived security problems at the lab. Those announcements that were made were never put into the directives

which actually govern the relationship between the Department and its contractors.

Mr. STUPAK. We have just seen a $350 million review, and things that were supposed to be done were never implemented at Los Alamos.

Mr. SELL. What we are doing, with the changes that we have made, is putting them into the directives which actually govern the contractual relationship so——

Mr. STUPAK. Let's talk about the directives though. You personally travel to Los Alamos. You did a memo on November 8 directing each laboratory and DOE facility operating a classified computer—didn't do anything about unclassified—but classified computer system to conduct an immediate and thorough examination to ensure that classified information is protected using multiple layers of cybersecurity. But isn't it also true that in this memo you set forth minimum standards that must be met by January 15, 2007; is that correct?

Mr. SELL. That is correct.

Mr. STUPAK. Were these minimum standards accomplished by January 15?

Mr. SELL. Not in all cases.

Mr. STUPAK. Not in all cases.

Your memo also says steps are to be taken—I am looking at your memo. I am sure you have one there in front of you. Steps to be taken are to include at a minimum those in the attached guidance prepared by DOE Chief Information Officer. There it is. So these were the minimum things.

Did anyone at Los Alamos come back to you and say, Mr. Secretary, you asked for the minimum. We went over and above; we went beyond the minimum. Did they do anything beyond the minimum? Any recommendations going beyond the minimum?

Mr. SELL. Yes, Mr. Chairman. The lab is doing a number of things beyond what was addressed in the memo. The memo that I put out was based on the immediate recognition that we had a real problem——

Mr. STUPAK. Sure.

Mr. SELL. Specifically with ports; I wanted to take the lesson that we had learned under very unfortunate circumstances at Los Alamos——

Mr. STUPAK. But you said part of it was complied by or complied with your request by January 15; other parts were not, correct?

Mr. SELL. To clarify completely, Los Alamos was the last of our labs and facilities to come into compliance, and that occurred on January 22. But that is a report that I have.

Mr. STUPAK. Well, let me ask you this question then. Your Chief Information Officer of NNSA in staff interviews said that she sent the team out on January 8 to see whether Los Alamos was complying with your directive. They found widespread noncompliance with your directive; isn't that correct?

Mr. SELL. I know as of January 8 the lab was not in compliance.

Mr. STUPAK. OK. Isn't it also true that even in the face of all the publicity of the most recent security lapse, that NNSA had to pull the entire team back from the lab because they either could not understand your directives or simply were incapable of responding to

your directives of securing the very areas and items that were under question as a result of the October 6 event? Why did NNSA have to pull back its teams?

Mr. SELL. Mr. Chairman, we are trying to deal in a very serious way; I gave out in this case very clear guidance as to what was to be accomplished. I could have just given clear guidance and gone on and done something else, but we followed up on that clear guidance by sending a team out.

Mr. STUPAK. And have you pulled back?

Mr. SELL. We sent the team out even before the deadline for compliance, and we found out when the team was out there that we weren't making progress——

Mr. STUPAK. We were not making progress?

Mr. SELL. We were not making progress at a sufficient pace to accomplish what needed to be accomplished by January 15. That came to our attention. We gave further direction. I clarified. I talked to the lab Director. They understood what their requirements were. We sent a team back out shortly after January 15 and concluded approximately January 22 that they had complied with the directive.

I think it is indicative that unfortunately ensuring compliance and making progress requires continued effort. It requires vigilance. It requires follow-up. It will require that long after I am gone. I only have control of the 2 years that I remain in my position, and that is the way I intend to deal. And I hope we can also institutionalize the progress that we are making, and there are a number of means within our disposal to help do that, through the contract, through the outstanding career staff that we have in our Department, through a number of the individuals and leaders of the laboratory that will remain into the next administration.

But it is difficult. There are reasons sufficient progress has not been made in previous years, and the only thing I can commit to you is that I am trying to deal in a way which is distinct and different and distinguishable from the ways that folks have dealt in the past.

I believe the Secretary and I have taken more aggressive action, and because I believe we are acting differently, at least I have some reasonable expectation that this time we will get different results, but only time will tell.

Mr. STUPAK. All right. My time has expired.

Mr. Whitfield for 5 minutes.

Mr. WHITFIELD. Thank you, Mr. Chairman.

And, Secretary Sell, we enjoyed your testimony today and appreciate your being here. It seems to me the years that I have been on this subcommittee and this issue of security breaches has been a subject that ultimately the effectiveness of really dealing with this is through the M&O contract. And you were involved in preparing or negotiating this most recent M&O contract with the consortium that is now operating LANS; is that correct or not correct?

Mr. SELL. I am happy to have the opportunity to tell you my exact level of involvement.

When I came to the Department in March 2005, the procurement work was already well under way. But certainly I knew it to be and

believed it to be the most important procurement—and I said this—in the history of the Department to date.

I am not the selecting official.

Mr. WHITFIELD. Who is the selecting official?

Mr. SELL. The selecting official at the time, I believe, and I will ask was Tom D'Agostino, who is not yet confirmed as the Deputy Administrator for Defense Programs. He has been a career member of our NNSA team for a number of years.

Mr. WHITFIELD. So was he within the NNSA at that time?

Mr. SELL. Yes, sir.

Mr. WHITFIELD. So the NNSA has the responsibility for selecting?

Mr. SELL. The NNSA had the responsibility; Mr. D'Agostino, I believe, was the selecting officer. But the Secretary and I did spend time—once the decision had been made, after the decision had been made, we met by video teleconference with the Source Selection Advisory Board. We met at length with Mr. D'Agostino, and it is my view that the decision that the Department made was absolutely the correct one.

Mr. WHITFIELD. Now what is the length of the contract?

Mr. SELL. The length of the contract, I believe, Mr. Whitfield, is a 7-year initial period but could be extended to 20 years. And I may be off 1 or 2 years.

Mr. WHITFIELD. What is the approximate total value per year to the consortium for being awarded the contract?

Mr. SELL. The total value, in rough order, about $2 billion, or $1½ to $2 billion a year flow through the contractor.

Mr. WHITFIELD. One and a half to $2 billion?

Mr. SELL. The fee available to the contractor is on rough order $70 million a year. So that is the potential net to the contractor.

Mr. WHITFIELD. So would I be accurate or inaccurate to describe the $70 million as incentive pay that they can receive in addition to the base amount?

Mr. SELL. The $70 million, Mr. Whitfield, includes both the base amount and the incentive portion. I think that is the total fee, roughly, that is available to be paid to the contractor.

Mr. WHITFIELD. OK. Now, you would think that since the real problem is safety and security, that is one of the major problems, that the incentives apportioned to do that would be greater than $3 million out of a total of $73-some million incentives. What would be the explanation for not making that a greater amount?

Mr. SELL. Mr. Whitfield, I don't think I can say anything that you would find to be a great explanation. Although the next panel—and I don't mean to just kick this to Mr. D'Agostino, I do think he is more informed on that. But I will also state my belief that we have a greater authority to restrict and pull back award fee for failures beyond just the $3 to $6 million for the security.

Mr. WHITFIELD. Are you aware, yourself, of the amount of penalty assessed in the 2004 6-month shutdown or not?

Mr. SELL. I am aware that it was generally in the neighborhood of around $3 million for the failures in 2004.

Mr. WHITFIELD. So that was a penalty that University of California paid?

Mr. SELL. That was a fee reduction in the amount that they——

Mr. WHITFIELD. A fee reduction. OK.

Now, it is my understanding that in the most recent contract that the consortium agreed that the 21 key personnel committed—that they committed to stay for a minimum of 2 years, and after 6 months the Deputy Director has already left; is that true?

Mr. SELL. Yes, sir.

Mr. WHITFIELD. Has anyone else left of those 21 key people?

Mr. SELL. To my knowledge none of the other 21 key individuals have left.

Mr. WHITFIELD. But you all do have authority to assess a fee for the breach of that aspect of the contract, I would assume?

Mr. SELL. I believe we do. And the only reason I hesitate is these are actual decisions that must be made by the contracting officer of whom I am not. I am trying to state as clearly as possible my expectation and belief.

Mr. WHITFIELD. My time has expired.

Mr. STUPAK. The gentleman from Louisiana Mr. Melancon.

Mr. MELANCON. Thank you, Mr. Chairman.

Mr. Sell, I was just wondering if Los Alamos or your children are causing this premature gray hair.

Mr. SELL. Both.

Mr. MELANCON. Some of the thoughts that have run through my mind, is the DOE team, is it on site, or was it just sent and came back and made a report? And how long were they on site when they were there?

Mr. SELL. We have a Federal site presence of around 120 individuals that live there, work there, and deal every day as the Federal representative at Los Alamos. But there have been tens and tens of individuals from headquarters, from other locations around the complex, outside experts that have come for the various reviews and evaluations and recommendations since this most recent incident in October.

Mr. MELANCON. Is it feasible or possible—we are looking at a June deadline, I think Mr. Friedman had said, to try to ascertain where we were in compliance—that—do you think it would make any difference if we put the team back down there several days a week between now and that time to monitor it, to make it progress faster, to maybe sometimes even point out their deficiencies, which apparently they are not seeing readily?

Mr. SELL. Well, I think it may well help, but I want to emphasize that we have a team there that worked for me. I mean, they worked for the Secretary and I and the Administrator and on down the chain. And their responsibility is to ensure that the contractor is performing pursuant to the terms of their contract.

And in addition to that, we have other oversight groups from headquarters. And we have other oversight groups from the contractor that they have hired, and they will continue to go—I mean, it is going to take continuous vigilance and monitoring, and perhaps other groups consistent with your suggestion would be helpful as well in ensuring that we make an institutionalized progress at the lab.

Mr. MELANCON. The people that are on the DOE team or the people that are responsible from DOE to monitor security, are they the

same people that are there when the first breaches occurred and subsequent breaches?

Mr. SELL. Some of them. But we have made a change at the top of the NNSA. The new Acting Administrator then subsequently made a change in the person that is heading the site office at Los Alamos. And so we are trying to find the right kind of leadership that can ensure much higher levels of performance at the lab.

Mr. MELANCON. I have a general in Louisiana I can suggest, because it sounds like it is going to take more than just a manager out there.

And I guess that is the concern that I have is it appears to me—and this is new to me—that we have rolled a head or two, but the problem is the tail is wagging this dog. And I just—do you have any comments? I mean, how deep is our problem, or is our problem—is the problem at the upper levels or security at the lower levels?

Mr. SELL. Well, it has been suggested, Mr. Melancon, that we should shoot the dog, and I have to reject that suggestion in the strongest possible terms. We do have 12,000 individuals at Los Alamos that were there under the University of California. They are there under LANS and will continue to be there. They are the core capability of that laboratory. And I do believe that we have deep-seated issues that are going to take time. And I would suggest, with all due respect to our Inspector General, it will take longer than a year. It is going to take time to change.

But we do have an outstanding new leadership team in place, and I believe the LANS team is the right team to lead the lab. I believe Mike Anastasio is the right Director to lead the lab.

I believe we have a new Federal lead there on an acting basis, Dan Glenn. We have an Acting Administrator, in Tom D'Agostino. We are putting in place new policies that will actually be incorporated in the terms of the contract by which we can hold the contractor accountable, and we intend to use the authorities in that contract to the greatest extent possible to ensure compliance and institutionalization of progress.

That is our approach going forward, and if the tail continues to wag the dog, then the committee may properly question whether I am the right one to continue to provide leadership. But I have laid out our path as to how we are proceeding, and I am confident that we can make real progress.

Mr. MELANCON. Mr. Chairman, if I could be allowed one more.

Mr. Sell, I guess the last question that I have is when do you think we are going to get this dog into the kennel?

Mr. SELL. We have made in the last few months substantial progress. Just for example, we had—there were thousands of open ports on classified computers when this—the day this thing came to light.

I have some level of confidence, not supreme confidence, but some level of confidence that that situation has been rectified; it will stay rectified at Los Alamos. We are changing our processes, but it will take—so we will continue to make progress. But the nature of security, particularly at a place as dynamic as Los Alamos, is constantly evolving, and I don't think there is ever a point where we will reach where we say—where we can say we are done and

we need not worry about security anymore. We will have to be constantly tending the kennel door to make sure we have got the dog contained.

Mr. MELANCON. Thank you.

Mr. STUPAK. Mr. Secretary, let me assure you no one wants to shoot the dog. We want to put that dog on a diet and put him in a new kennel.

Mr. MELANCON. He needs to be trained.

Mr. STUPAK. Mr. Burgess, questions?

Mr. BURGESS. Thank you, Mr. Chairman.

Mr. Secretary, good to see you again. You mentioned in your testimony, or I think in response to a question, that you were not the selector in the process of going through the RFP last year. I have asked this question of other witnesses, but in your opinion the process was fair and open and above board?

Mr. SELL. Yes.

Mr. BURGESS. Let me ask you this: At Los Alamos what measures are being taken to ensure the laptops and removable media are being encrypted or sequestered so that sensitive data is not leaving your site unprotected?

Mr. SELL. Just so I understand, this is a different set of vulnerabilities as to the encryption of data that is then—you mean when it is communicated across open lines, or when it is in laptops?

Mr. BURGESS. Yes. Is it encrypted in laptops to reduce susceptibility to theft?

Mr. SELL. The encryption of classified material on laptops when they are at a secure facility is a matter that is covered under our policies, and those policies are those directives that—the manual which governs that is being updated and will be finalized in the course of the next few weeks. That governs the exact terms under which laptops have to be encrypted. But I am sorry, Dr. Burgess, I can't give a more exact recitation as to exactly how that is carried out.

Mr. BURGESS. And will that be something that is universal across the Department of Energy, or will that be specific for Los Alamos?

Mr. SELL. It will be universal across the Department.

Mr. BURGESS. We heard previous testimony from the other panel that the concept of at will employment be curtailed, but that really is not something that is within the purview of the Department of Energy, is it? That is up to the individual contractor involved?

Mr. SELL. That is something I believe that we largely leave to the contractor as to the negotiation of employment terms with their employees.

Mr. BURGESS. When the contract was awarded to LANS a year ago, it was done so in a belief that it could substantially improve security at Los Alamos. Do we still believe that?

Mr. SELL. I do.

Mr. BURGESS. And we believe we have in place the metrics by which we are going to be able to show not just this committee, but America at large that is indeed the case?

Mr. SELL. We have some metrics, and we are developing additional metrics, and we will develop even further ways of measuring progress once we have the full recommendations from our two

groups that are reviewing the IG's report and once we put in place all of the policies going forward. But certainly our ability to measure progress and understand when there are failures or when there are potential failures before they actually happen or before they get outside the gates of the laboratory is a very important management tool that we must have, and I will ensure that we will have it.

Mr. BURGESS. So in your opinion that is what real progress will look like? Hopefully to us it will look like the absence of breaches, and we won't be back here every 6 months covering one of these incidents.

Mr. SELL. It is—a much higher level of performance must be required. But I would like to just take a moment. I think some context about what our lab does. They generate many secrets. That is the nature of their business. That is the tools of their trade. And we talk about 139 vault-type rooms and 3,000 classified computers. That is the nature of the work that we do. And in order to print something or to move it around the lab or to store it, it requires lots of computer capability. It requires ports. It is a very complex manner dealing with our business. Vault-type rooms——

Mr. BURGESS. Can you then reduce the number of computers without compromising your business?

Mr. SELL. I don't know that we can. That is certainly something we are looking at, and I think it is a sound suggestion. It is a suggestion that has been made internally. But I have not received a recommendation that we, in fact, can do that. If we can, we will. But our business at Los Alamos is national security matters. Almost all of it is classified.

And so I just want to try to put this into context that it may not be as simple as taking 139 vault-type rooms and going to 100. That may mean that a third of the work that we would like to do can't get done.

Mr. BURGESS. Thank you, Mr. Chairman. I will yield back.

Mr. STUPAK. Mr. Sell, if I may, let me just ask you quickly, hopefully we are going to have the Secretary here in March to answer some questions, but he put out a memo on November 28 after this incident came to light, and he states that the recent incident at Los Alamos and the findings of the Inspector General report indicate there may be significant deficiencies involving the application of personnel security policies and standards within the Department. What were those significant deficiencies?

Mr. SELL. Mr. Chairman, I don't know that I can get into the details of the deficiencies without treading into areas which are governed by the Privacy Act in the instant case.

Mr. STUPAK. Will you stay for the executive session then? We can ask you the questions then?

Mr. SELL. I will accommodate the committee and you, Mr. Chairman, however you would like.

Mr. STUPAK. OK, because I had a couple of follow-up questions on that. So allow me to do that in closed session. Thank you.

Anyone else have questions? Mr. Whitfield.

Mr. WHITFIELD. Just one additional quick question. Mr. Burgess was asking questions about the number of computers. This is a similar question relating to the separate security area, over 1,700 of them, and I was just wondering have you yourself formed any

opinions about to believe that such a large number of geographically dispersed and classified areas increases the vulnerability of operations? And do you think the areas should be reduced? And your views on that.

Mr. SELL. Mr. Whitfield, I believe that there may be benefits from those, and certainly instinctively I would think that we could perhaps do that. I know that there are views inside our Department that we can do that. We are looking at it. And I know in your letter of last night you suggested also that we look at it, and we will do that. We are looking for suggestions and good ideas from any corners from which they come.

I have not made a conclusion that is going to be possible. But it may well be.

Mr. WHITFIELD. Thank you.

Mr. STUPAK. Thank you, Mr. Secretary. And, yes, sir. You want to clarify something?

Mr. SELL. Well, Mr. Chairman, I wanted to take an opportunity to answer a question which you posed to other witnesses but you did not pose to me: What is unique about Los Alamos?

Mr. STUPAK. The unique mission that they do there. What is the unique mission that cannot be duplicated at any of our national labs?

Mr. SELL. Los Alamos National Laboratory and the men and women of that lab invented and designed and are responsible for certifying to this day two-thirds of our strategic nuclear weapons stockpile. They are the only place in the country today where we can build a plutonium pit, which is the trigger, in layman's terms, for a nuclear weapon. They have many, many other unique capabilities beyond that.

But it is my view that we have to have Los Alamos, and we have to be successful, but more importantly that we can be successful. We are not destined to failure. We can be successful, but it is—we must have it.

Mr. STUPAK. No doubt men and women at Los Alamos are unique. Whether they work in Sandia, Los Alamos, or Lawrence Livermore, they are all unique and all talented people, and we have no problem with that. But we are not going to continue to have lapse after lapse. They owe it to the American people, not this committee, but the American people, to guard.

You tell about the most sensitive things that are going on not only for nuclear or antiterrorism or anywhere else. We cannot have it going on at the same time going out the back door. That is what we want to impress upon not only you, but the Secretary and everybody else.

Look at the list here, how many hearings we have had here? 350 million taxpayer dollars spent; the fine was $3 million, less than 1 percent? No wonder there is no accountability. They will just ignore it and continue.

We just want things done and done properly. American people deserve it. It is the American people who pay for those weapons, American people that have developed this. And we appreciate everyone who works at those labs, but it is not going to continue like it has been.

With that, if you have any further comment?

Mr. SELL. Mr. Chairman, I agree with your final statement completely, and you have my full commitment for as long as I am in my position.

Mr. STUPAK. We appreciate that, and we look forward to talking to you a little bit more in executive session. Thank you.

Mr. STUPAK. We have our third panel. Our final panel consists of five people: Mr. Thomas D'Agostino, Acting Administrator, National Nuclear Security Administration; Ms. Linda Wilbanks, Chief Information Officer, National Nuclear Security Administration; Michael R. Anastasio, Director, Los Alamos National Laboratory; Mr. William Desmond, Associate Administrator and Chief for Defense Nuclear Security; and Mr. Thomas Pyke, Jr., Chief Information Officer, Department of Energy.

It is the policy of this subcommittee to take all testimony under oath.

Please be advised the witnesses have a right under the rules of the House to be advised by counsel during testimony. Do any of the witnesses desire to be advised by counsel at this time? If so, would you please introduce your counsel?

Hearing nothing in the affirmative, I take it you do not have counsel with you.

Please rise and raise your right hand to take the oath.

[Witnesses sworn.]

Mr. STUPAK. Let the record reflect all witnesses answered in the affirmative.

Mr. D'Agostino, sir, is going to start, please.

**TESTIMONY OF THOMAS P. D'AGOSTINO, ACTING ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION**

Mr. D'AGOSTINO. Thank you, Mr. Chairman. My name is Thomas D'Agostino, and I am the Acting Administrator of the National Nuclear Security Administration within the U.S. Department of Energy, a position I have held since January 20, 2007. I am also the Deputy Administrator for Defense Programs.

I want to personally assure you that with respect to the current issue of security at Los Alamos National Laboratory, that we are committed to providing the most effective security possible for nuclear weapons, nuclear material and classified information both at the laboratory and at each of our NNSA facilities.

The primary reason I am acting as Administrator is because of the Secretary of Energy's dissatisfaction with the continuing series of security incidents. When the Secretary does not see results he expects, he takes action. The most recent of these was his request for the resignation of the former NNSA Administrator, Linton Brooks.

Mr. Chairman, the Secretary and the Deputy Secretary expect me to be active in running the NNSA and to be accountable for our performance and make decisions when they need to be made. That is exactly what I am doing.

I have made it clear to Los Alamos National Security, or LANS, the contractor who manages the laboratory, that we are expecting them to take appropriate action against any LANS employees determined to be accountable for most recent security incident. LANS

has reported that formal disciplinary action will be taken against 24 employees.

I have decided to spend my first 2 days on the job as Acting Administrator in New Mexico both visiting the laboratory itself and the Federal site office responsible for overseeing the laboratory to get firsthand, upfront and personal information that I can use. I did that last Monday and Tuesday.

I stressed to them my expectations concerning oversight of the laboratory activities and the importance of accountability and meeting our commitments.

I've directed that Dan Glenn, one of the Department's most experienced site office managers from the Pantex site in Texas, to serve as the acting Federal site office manager until a permanent replacement is found. Mr. Glenn has extensive nuclear safety and security experience at our most sensitive site. In fact, Pantex is the only NNSA facility where we have complete nuclear weapons on site. Dan has my complete confidence.

Dan spent last Thursday and Friday at Los Alamos assessing current activities and operations at the Los Alamos site office, and he is assembling a team to aggressively oversee laboratory security and safety programs and to recommend not only immediate, but near-term fixes, fixes that we can implement and take action on right away. Dan will take over Los Alamos site office on February 5.

With respect to our specific interactions with LANS, management and operating contractor on the latest security incident, all contractual options for both penalties and motivation are under consideration and on the table. I want to assure you that this is not an academic exercise. With a nominal fee at stake, the maximum available annual fee with security and safety as key factors is over $70 million. The majority of LANS's fee is at risk, as is their ability to earn additional award terms—or years—added on to the contract. The combination of award fee and award term are very powerful incentives on performance, and I intend to fully utilize these tools that are available to me in managing this contractor.

The Department is also conducting a review of the incident to determine whether notice of violation will be issued, as was discussed earlier.

Finally, the contract has a clause called Conditional Payment of Fee, Profits, and Incentives. This clause allows for the complete elimination of fee in the event of serious safety or security events that result in a loss of life and irrecoverable harm to the security of the United States.

On January 3, 2007, we took further direct action and unilaterally notified the LANS Board of Governors Executive Committee that I was calling a session in Washington the following week. On January 10, I met with the executive committee and told them of my specific concerns on how they have handled the current security incident at Los Alamos and my expectations for performance. The Secretary and the Deputy Secretary joined me to emphasize the seriousness of the situation.

The executive committee will provide me with their plans on how they will address the current situation and improve the culture at

the laboratory. In the coming months I will be routinely meeting with members of the executive committee to hear how they are progressing with their plans. Additionally, I have asked the chairman of the committee, Mr. Gerald Parsky, to call the Secretary on a regular basis, probably monthly, maybe more like on a 5-week basis, to update him personally on the actions that the board is taking to reach back to the corporate parents and to support improvements at the laboratory.

In closing, Mr. Chairman, I commit to you that if the current laboratory management team is unable or unwilling to change the security culture at Los Alamos, I will use every tool available to me consistent with the terms of the contract to effect the kind of positive changes I expect and we deem necessary for our taxpayers.

Thank you, and I would be pleased to take any questions the committee may have.

[The prepared statement of Mr. D'Agostino appears at the conclusion of the hearing.]

Mr. STUPAK. Mr. Desmond, your opening statement.

Mr. DESMOND. Mr. Chairman, I do not have an opening statement.

Mr. STUPAK. Ms. Wilbanks, opening statement.

**TESTIMONY OF LINDA WILBANKS, CHIEF INFORMATION OFFIER, NATIONAL NUCLEAR SECURITY ADMINISTRATION**

Ms. WILBANKS. Chairman Stupak, Ranking Member Whitfield and members of the committee, good afternoon. I am Dr. Linda Wilbanks, the National Nuclear Security Administration Chief Information Officer.

Thank you for the opportunity to discuss the cybersecurity incident at Los Alamos National Laboratory and the actions NNSA has taken to prevent similar incidents. As CIO, I am responsible to the Administrator for cybersecurity, specifically policies and procedures to ensure the security of the information and technology as it relates to the NNSA mission and to enhance our ability to protect the classified, sensitive and unclassified information systems.

I came to NNSA after almost 3 years at Goddard Space Flight Center as a CIO. I have over 30 years experience in information technology, a bachelor's degree in mathematics, a master's degree in engineering and a doctorate in computer science.

When the recent incident was reported, at my direction the NNSA Cybersecurity Program Manager and the Director of the Diskless Workstation Task Force immediately flew to Los Alamos with two members of the DOE cybersecurity team. Their objective was to learn as much as possible about the incident from the cybersecurity perspective and determine if any of the contributing factors could put LANL at further risk or they could take place at other NNSA sites.

I also traveled to Los Alamos and met with the cybersecurity personnel responsible for the Los Alamos computer systems to further understand the issues. We quickly identified two issues: the accessible USB ports and the cybersecurity plan that did not address the specific risks of the system and was incomplete, which contributed to the system's vulnerabilities.

The Los Alamos incident occurred when a trusted insider maliciously decided to use a personal device to electronically remove classified material. The cybersecurity plan allowed for the cages to be unlocked with exposed USB ports because the servers were in a secure room with limited access by people with clearances to access the classified material.

As a result of this incident, we have taken a number of actions to strengthen the cybersecurity at Los Alamos and all NNSA sites addressing the cybersecurity root causes that allowed this incident to occur.

As a result of the incident, I immediately required that all NNSA sites identify the open ports on classified systems and determine if they needed to be open or could be permanently disabled.

We purchased an enterprise license for software to monitor open port activity. All sites, including Los Alamos, are now in compliance with any ports that can be used to transmit data being sealed or monitored.

The Designated Approving Authority, the DAA, is responsible for approving an IT system for operations by signing the cybersecurity plan that states how the system will be in compliance with DOE and NNSA policy. I have temporarily reassigned the DAA from the Sandia site office to Los Alamos to strengthen the cybersecurity there. I have directed the DAAs at all NNSA sites to review the cybersecurity plans, and I hold them accountable to ensure that those plans now address the specific risk of each system and to identify and rewrite the plans with omissions such as those that allowed the incident at Los Alamos.

I have increased the funding to Los Alamos to hire three cybersecurity experts to support the Federal activity there. I have assembled a team of eight cybersecurity experts from headquarters and NNSA and had them inspect all the vaults at Los Alamos to determine if they were in compliance with the Department's directive to close ports. The team initially found areas of noncompliance; however, when reconvened on the site this past week, they inspected all vaults and are now in compliance.

I further directed the team to inspect the cybersecurity implementation at all NNSA sites. Those inspections will start in February and conclude in April when the team revisits Los Alamos.

My office has worked with the DOE CIO, Mr. Tom Pyke, to identify areas where policies and procedures are needed to strengthen cybersecurity and to aggressively implement them as quickly as possible. NNSA is responsible for over 70 percent of the classified networks within the Department. We take this responsibility very seriously, and maintaining the security of the classified networks is our highest priority.

Because of the dynamic nature of cybersecurity, no one can guarantee there will never be another cybersecurity incident at any NNSA site. It is not possible to have perfect and complete security. We live in a world where hacking into Federal systems is a hobby of many students and many highly paid professionals. We are using every tool available and have put in place strong cybersecurity policies to ensure this type of event does not happen again.

NNSA is working very diligently to maintain a secure environment for our information and that of the Department. We work closely with our sites to identify the risks, and we are moving ahead in many areas, and we are making progress.

I am happy to answer your questions, sir.

[The prepared statement of Ms. Wilbanks appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you.

Mr. Pyke.

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

Mr. PYKE. Good afternoon, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer at the Department of Energy. I came to the Department in November 2005 and have given a high priority to revitalizing the management of cybersecurity within the Department.

Over the last year, DOE has undertaken a major effort to improve our cybersecurity. We developed a plan to update departmental cybersecurity directives and to issue guidance in specific high-priority areas. In December 2006, the Deputy Secretary signed a new DOE cybersecurity departmental order which established a new governance structure for cybersecurity program manager. The order directs the use of a risk-based management approach and makes clear assignment of responsibility to the Under Secretaries and other senior officials to oversee cybersecurity management within their organizations, including the field organizations under their jurisdiction.

The Under Secretaries have accepted this enhanced role and are working hard to strengthen the management of cybersecurity. This order is a key part of the institutionalization of forceful new direction to the Department. As referred to earlier by Deputy Secretary Clay Sell.

The new order provides for timely issuance of urgently needed cybersecurity guidance. To date, I have issued 20 cybersecurity guidance documents, and the Office of the Chief Information Officer continues to develop guidance in accordance with the plan developed last year. I have already issued guidance on certification and accreditation of systems and on system configuration management, both directly relevant to the recent Los Alamos incident. We have also issued special guidance on the protection of personally identifiable information and on the disposal of disk drives.

Finally, directly to the concerns being addressed at this hearing, we have recently completed a planned DOE National Security Systems Controls Manual. It is now in final review in the Department. We have been able to incorporate actions in the manual based on a number of the lessons learned from this incident.

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

[The prepared statement of Mr. Pyke appears at the conclusion of the hearing.]

Mr. STUPAK. Mr. Anastasio.

**TESTIMONY OF MICHAEL ANASTASIO, DIRECTOR, LOS ALAMOS NATIONAL LABORATORY**

Mr. ANASTASIO. Chairman Stupak, Ranking Member Whitfield and other members of the subcommittee, I thank you for the opportunity to speak with you today.

I'm Michael Anastasio, and since June 1, 2006, I have been the Director of the Los Alamos National Laboratory. I am also President of the laboratory's new management company, the Los Alamos National Security, LLC, often referred to as LANS. Previously, I served our country for over 25 years at the Lawrence Livermore National Laboratory, first as a scientist and ultimately as the director of that institution.

The security breach at Los Alamos National Laboratory is deeply troubling. I want to make it absolutely clear to all of you that my board and I personally find this incident totally unacceptable. It is precisely because of such incidents that the DOE made its decision to recompete the contract at the laboratory.

I want to talk with you today in my opening comments about four main points: First, that we take this incident very seriously, that we took immediate action upon learning about the issues, that we bring a different approach to running this laboratory, and that this incident accelerates our plans to develop a robust security system that handles today's issues and anticipates the future.

Although this incident occurred only weeks after we took control of the laboratory, I am responsible for this incident. But even more importantly, we are responsible for the solution to fix the laboratory with regard to security and other matters. I have detailed in my written testimony a number of corrective actions that we've taken, and I would just like to cover six of those right now.

We have tightened controls on the ports on all the classified computers. Through our parent organizations, we have tapped into independent security expertise from across the country. We have established a new cybersecurity organization that reports directly to me. Our guard force has significantly increased the number of searches of laboratory personnel as they leave the site. We terminated the relationship with the scanning subcontractor, and I have disciplined 24 employees of the laboratory as a result of this incident. We are prescreening for illegal drugs of all new hires and will be randomly testing the existing workforce.

These steps have already proven effective as we heard DOE and NNSA have certified last week that all the vault-type rooms that we have at the laboratory with classified computing are now compliant. But these initial actions aren't sufficient. We must move beyond the quick-fix, Band-Aid approach that's been used in the past, and that means we must now have—address security in a comprehensive and integrated manner that anticipates risks associated with the inexorable advancement of technology.

There will not be a silver-bullet solution because there are none, but we have developed a forward-looking approach addressing all of the elements of enhancements to the security that needs to be done and do them simultaneously. We will quickly put in place demonstration projects that create a test bed to try out all these new security approaches that we have in mind. We will consolidate 10 to 20 of our existing vault-type rooms into one overall facility.

In there, we will implement clear policies with advanced technologies and proven behavioral methods. In this way, we will have a plan that we have demonstrated will work and that we can then implement across the entire laboratory.

So, Mr. Chairman, in conclusion, the steps that I and the board are taking are a fundamental break from the past. The LANS partnership brings together expertise and successful performance from across the Federal and the commercial sectors.

As president of LANS, I report to a very demanding board, a board that provides a level of oversight, engagement and rigor that this laboratory has not seen before. I have a brand new management team that I, personally, selected from across our parent companies. The partnership of these four companies gives me a deep bench of capabilities and personnel that I'm already tapping into.

I'm already seeing evidence of positive change at the laboratory, and in time these steps will lead to dramatic improvement in the overall performance of the laboratory. We have taken immediate action. We have an ambitious and comprehensive plan. We have extraordinary capabilities to draw upon, and we are working aggressively to execute our plan. All of my leadership team and I, personally, are deeply committed to the Los Alamos National Laboratory's success and its essential role in protecting our country's national security.

Thank you, Mr. Chairman, and I look forward to answering all of your questions.

[The prepared statement of Mr. Anastasio appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you. And thank you all for your testimony.

Mr. Anastasio, you said you are responsible for what happened at Los Alamos. Then what's been the consequences of accepting that responsibility? Has anything happened to you?

Mr. ANASTASIO. Has anything happened to me?

Mr. STUPAK. Yes.

Mr. ANASTASIO. I've been working a lot longer hours, sir. Do you mean if I've been disciplined in any way?

Mr. STUPAK. Yes.

Mr. ANASTASIO. I've been certainly in contact with my board from the very beginning of this incident, and they've made their expectations very clear to me. The board also talked with NNSA and the Secretary, and based on that conversation, they've passed along those expectations, and I've heard the same from the Department as well, personally. It's been very clear to me what everyone expects of us at the laboratory, and——

Mr. STUPAK. Well, what are the lessons you have learned since then, and what is being done to ensure this incident doesn't happen again?

Mr. ANASTASIO. Well, as I tried to detail for you a little bit in my oral testimony and more so in the written, it's that we've taken a number of aggressive actions.

Mr. STUPAK. Such as?

Mr. ANASTASIO. As soon as I learned about this incident, within hours we had already started to control the ports on classified computers. We started taking that action immediately.

Mr. STUPAK. We've heard that since 2000. We've had eight hearings on cybersecurity since we first brought it up in 2000, so excuse me, but I don't—what's going to be different? We've heard all this before. This is my eighth hearing now on this.

Mr. ANASTASIO. We have actually succeeded in doing that, and the recent audit confirms that, in fact, we have complied with all the direction we've been given.

Mr. STUPAK. The audit from the Inspector General, Mr. Friedman, said the core security at Los Alamos is in shambles, the core security. I'll read it for you exactly if you want it, because I asked him about it, and it was the very basis of Los Alamos; the very core of their security was not good.

Mr. ANASTASIO. Mr. Chairman, I find this incident and the issues around it totally unacceptable. My board finds that totally unacceptable. They're going to hold me accountable to fix this.

Mr. STUPAK. And we find it totally unacceptable.

What are we going to do to fix it?

Mr. ANASTASIO. I understand that, and we are in the process of doing that. And so we've taken a series of immediate actions which, I think, address the immediate concerns and risks at the laboratory; and, at the same time, we have a long-term plan that will get us to a point where we can be out in front of these issues—not always playing catch-up that we've done in the past—and that will allow me and the American people and you, the Congress, to have confidence in this laboratory again.

The Department recompeted this contract, we understand, very well. They recompeted this contract because of these issues, and I understand that the reason I've been brought in and my team and this new contractor is that we need to fix these and the other issues that are going on at the laboratory. And that's what I'm here to commit to you to do.

Mr. STUPAK. The Inspector General's report I will quote now,

> Our review revealed a serious breakdown in core laboratory security controls. In short, these findings raise serious concerns about the laboratory's ability to protect both classified and sensitive information systems.

So that's the challenge you have.

Ms. Wilbanks, at Los Alamos, sensitive, unclassified computer systems, are they adequately protected from today's threat? You mentioned hackers always trying to get in.

Ms. WILBANKS. The unclassified, sir?

Mr. STUPAK. The unclassified. "Sensitive, unclassified," they're called.

Ms. WILBANKS. While we do not put as much attention on those systems as we do the classified systems, sir, I do believe they are adequately protected. The 25,000 systems that were referred to by Mr. Podonsky, they are C&A'd under the NIST provisions.

Mr. STUPAK. Sure. Would you bet your job on that all 25,000 are secure?

Ms. WILBANKS. I can't guarantee what a hacker will do and what the new technology will be, sir.

Mr. STUPAK. OK.

Ms. WILBANKS. I am doing everything in my power, sir, to make that guarantee to Mr. D'Agostino.

Mr. STUPAK. OK. In your testimony, you state "We have since secured all USB ports at all NNSA sites and are reviewing all cybersecurity plans to ensure they address the specific risks for that system. This type of incident, the undetected transfer of classified information to a portable device, could no longer occur at any NNSA site."

So let me ask you: Why wasn't all of this fixed prior to this incident?

Ms. WILBANKS. Actually, at some of our sites, sir, it was fixed.

Mr. STUPAK. Right. But not at all of them, obviously.

Ms. WILBANKS. That is correct, sir. At a meeting of all of the DAAs from the sites in November, the "open ports fine" issue was brought up.

Mr. STUPAK. Sure, that's November, but wasn't that really one of the primary reasons the lab was shut down in July 2004?

Ms. WILBANKS. I was not here then, sir. I'm sorry.

Mr. STUPAK. Did you ever review the report in 2004 and see what was required for cybersecurity at the lab's computers?

Ms. WILBANKS. Yes, I did, sir, and there was very minimal in there for cybersecurity.

Mr. STUPAK. OK. Hopefully, I'll have some time for some follow-up because I would follow that up, but my time is up.

Mr. Whitfield.

Mr. WHITFIELD. Thank you, Mr. Chairman, and I thank the witnesses for their testimony today.

Mr. Anastasio, you were the Director of Lawrence Livermore, I think you said in your testimony.

Mr. ANASTASIO. That's correct, sir.

Mr. WHITFIELD. For how many years?

Mr. ANASTASIO. Almost 4 years.

Mr. WHITFIELD. And you've been here now for about 7 months at Los Alamos?

Mr. ANASTASIO. Since June 1, that's correct.

Mr. WHITFIELD. Well, you might have some unique perspectives on this that we've been asking a lot of people, and I read this comment that said LANS' volume of classified holdings is unnecessarily large, conducted in too many security areas, involving too many people, and is spread out over too large of an area.

Would you agree that that assessment may give a synopsis of the primary differences in Los Alamos and Lawrence Livermore and would explain why security is such a challenge at Los Alamos?

Mr. ANASTASIO. Well, I would agree those factors add a challenge to Los Alamos, but I believe the—one of the fundamental issues at the laboratory right now is that there is unclear, complicated policies which are inconsistently applied across the laboratory. And of course one of the reasons for inconsistency is the fact that there are so many different locations. But in the past, the laboratory has—each organization has implemented their own version of the overall policies, which led to inconsistency; and I would also argue that the policies are overcomplicated and sometimes inconsistent, so we have not been enabling our employees to be a success. What they see is confusing. They don't know what is allowed and what's not allowed. So that's one of the things that was in the core approach that we've taken to fix the laboratory. But at the same time, we

are also looking to consolidate the number of vaults, to bring those down. The laboratory, before we arrived, has done a lot to reduce the total number of accountable, removable, electronic media, a number of documents, so I think these are all approaches to an overall plan that we're putting together.

Mr. WHITFIELD. So, the confusion in policy, is that partly the responsibility of the Government and the holder of the M&O contract?

Mr. ANASTASIO. Well, certainly, we are driven by the policies that come from the Department through our contract, but I believe my responsibility goes beyond that.

My job is to make sure the laboratory is secure. I have to be compliant with the policies, but if that is not sufficient, I have to take further action. I believe that——

Mr. WHITFIELD. But you found a lot of things wrong with the policy and the confusion in the policy when you arrived there. I mean there obviously was room for improvement.

Mr. ANASTASIO. Yes, there's certainly room for improvement, and we're off dealing with that and trying to——

Mr. WHITFIELD. Now, why would we expect that there would really be a great improvement when the University of California had responsibility for 64 years prior to the new M&O contract, and now they are a 50-percent stakeholder in the new contract?

Mr. ANASTASIO. Well, I think there's a number of reasons why you should have confidence.

This is a new team. First, we have a board of directors that we've never had before who are very demanding.

Mr. WHITFIELD. And who is on the board of directors?

Mr. ANASTASIO. There are 11 members of the board of directors—six from the parent companies and five from the outside—outside world.

Mr. WHITFIELD. And the parent companies would be the University of California, Bechtel, and who else?

Mr. ANASTASIO. BWX Technologies and Washington Group International.

Mr. WHITFIELD. Now, what is the Washington Group International? Who is that?

Mr. ANASTASIO. I'm sorry. I'm not sure what you mean by that.

Mr. WHITFIELD. I'm not familiar with that.

Mr. ANASTASIO. The president of that is Presray.

Mr. WHITFIELD. What is the experience of that company? Where does that come from?

Mr. ANASTASIO. Oh, they are involved, for instance, with the Savannah River site. They are a major part of that contract. They are at the WIPP site. Those are a couple of places. They have a lot of expertise in nuclear—nuclear facility management.

Mr. WHITFIELD. But the board is composed of six members from those four entities?

Mr. ANASTASIO. That's correct, sir.

Mr. WHITFIELD. And then five members outside of those?

Mr. ANASTASIO. That's correct.

Mr. WHITFIELD. Who selected the board members, the five that are outside?

Mr. ANASTASIO. The six members on the inside from the companies, yes.

Mr. WHITFIELD. OK, and those five, what companies do they represent?

Mr. ANASTASIO. We have one for oversight from PricewaterhouseCoopers for financial oversight. We have someone from Stanford. We have a former admiral, et cetera.

Mr. WHITFIELD. And the board meets how often?

Mr. ANASTASIO. The board normally meets quarterly but whenever they need to. So we've had quite a number of meetings, both formal meetings—but I'm in constant conversation on the telephone with the key members of the board whenever that's necessary.

Mr. WHITFIELD. Now my time has expired. I just have one quick question.

As a result of the most recent breach, the 1,500 and some documents that were a problem, as the director of Los Alamos, representing the president of the new consortium, would you expect that the Government would penalize your company financially for that breach?

Mr. ANASTASIO. Oh, I certainly understand that part of our fee or, ultimately, all of our fee could be at risk for this or any other incidents that go on at the laboratory. We understand that very well.

Mr. WHITFIELD. OK. Thank you.

Mr. STUPAK. The gentlewoman from Colorado.

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

Mr. Anastasio, I wanted to follow up on some of the ranking member's questions because you successfully ran Lawrence Livermore for a good number of years, and I'm wondering if you could just tell me very briefly what is it that's so different at this facility. You said a minute ago there's unclear competing policies that are applied inconsistently. Are there other things?

Mr. ANASTASIO. Certainly things that the ranking member identified are issues as well, the fact that it's physically spread out——

Ms. DEGETTE. The physical layout.

Mr. ANASTASIO. Also, there's a history at the site of each organization having a lot of autonomy to implement the specifics in their own work area. All of these things lead to some of these challenges that we face.

Ms. DEGETTE. How's the morale out there?

Mr. ANASTASIO. Well, the morale of the employees—they are really—I think it's improving. They've been through a lot of controversy over the last years. They understand, because of the contract competition, that change is happening and it needs to happen, and I think they're very, very committed to their mission.

Ms. DEGETTE. Do you think that they're committed to complying with security procedures?

Mr. ANASTASIO. I think the employees are very committed to do their job very well, including their security responsibilities.

Ms. DEGETTE. And is that a change in attitude? Well, you've only been there since June.

Mr. ANASTASIO. Yes. I can't say how much there's been a change in attitude.

Ms. DEGETTE. I'll be frank. When we were out there a couple years ago, when Mr. Barton and I were there, we got the sense that part of the problem was that many of these high-level employees felt like these were—these security procedures were ridiculous, and they didn't really want to comply. Have you found some of that attitude?

Mr. ANASTASIO. The attitude I found is, first, a very loyal commitment to their country and their mission but also a confusion about what standard they're being held to. And so they want to comply, but they're not clear what they're supposed to——

Ms. DEGETTE. And this is what you were talking about, the unclear, competing policies applied inconsistently?

Mr. ANASTASIO. Yes. And I think one of the things we're trying to do is, as we define the overall goal and policy we want them to achieve, we're trying—we're involving some of the employees in developing the implementation plan. That way, they're there from the beginning. Now, they don't get the final choice of what that plan is, but they're part of that discussion so they understand why the policy is in place and how it's implemented.

Ms. DEGETTE. Right. Let me ask you this. Mr. Friedman said that he felt like we should give the agency until June, which would be your 1-year anniversary, to fix this.

Can you fix all of these problems by June, and are you willing to commit to that today?

Mr. ANASTASIO. I would agree with the deputy director that we are off fixing them right now. We have been fixing these problems ever since the incident occurred, that we are making progress every day.

Ms. DEGETTE. OK. My question is can you do it by June, "yes" or "no."

Mr. ANASTASIO. I think this is a continuous challenge that we have to be on top of every day from now until——

Ms. DEGETTE. Can you make substantial progress by June?

Mr. ANASTASIO. Absolutely, we can make substantial progress by June.

Ms. DEGETTE. OK. Thanks. I just have a quick question for you, Mr. D'Agostino.

In the binders of this Fiscal Year 2000 Performance Evaluation Plan—I'm sure you're familiar with that plan——

Mr. D'AGOSTINO. Yes, ma'am.

Ms. DEGETTE. In part of that plan on page 5 is performance-based incentives. We're a little confused up here. Mr. D'Agostino testified about everybody now understands that there are incentives under this new contract.

We're a little concerned about, if we wanted to take some kind of punitive action if these problems aren't fixed, how much we could penalize the management by. Is it the entire $73,280,000 or some other number of that?

Maybe you can quickly explain that to me.

Mr. D'AGOSTINO. Yes, ma'am. Thank you for the opportunity to do that. A couple of points.

The one is there's the clause I mentioned during my oral testimony, conditional payment of fee. It puts that whole $73 million at risk.

Ms. DEGETTE. OK. So, if we wanted to, we could penalize them that whole amount?

Mr. D'AGOSTINO. Yes, ma'am, but there are conditions associated with the contract, associated with the level of severity and——

Ms. DEGETTE. Whose department is that?

Mr. D'AGOSTINO. I would go through the contracting officer, is my——

Ms. DEGETTE. Who determines the level of severity?

Mr. D'AGOSTINO. There would be an analysis done. The damage assessment, for example, in this particular incident will be looked at. If there are further safety and security problems that happen, those would get added up into the problem, if you will, when we look at fee determination at the end of the fiscal year.

So what we will do at the end of the fiscal year, which is September 30 of this year, take a look at the laboratory's performance not only on this particular security incident but on whether there have been any safety issues associated with the laboratory, and look at whether that conditional payment of fee clause actually applies here.

In addition, your question, ma'am, was referring to this particular page which which broke down the $70-plus million. There is the fixed fee: 30 percent of about $22 million; and the incentive fee. Within the incentive fee that you call out "performance-based incentives". There are very specific measures and deliverables under each one of those performance-based incentives 1 through 13. PBI No. 5 applies to safeguards and security, which was pointed out earlier that, if it's only $3 million of the whole 70, why is that—why should we feel——

Ms. DEGETTE. Right. So do you think we can only penalize them $3 million or $73 million?

Mr. D'AGOSTINO. No, ma'am. All of the $73 million is at stake. I wanted to get to a point. I did spend the first few days of this job at Los Alamos last week. I got a chance to see firsthand the conditions that we've talked about earlier in the hearing.

Based on that, I directed the manager at the site office, working with Mr. Desmond, to reevaluate, and we are unilaterally reevaluating this fee allocation within this particular plan. So we have two approaches, and we will—as I mentioned in my testimony, I'm going to make full use of the contract because that is the main tool. It is the tool that we should use and will use in order to make sure that the message gets across to the contractor.

Ms. DEGETTE. OK.

Mr. D'AGOSTINO. I apologize for taking so long. We are going to conduct a reevaluation of this allocation, and we will be working with LANS on that reallocation, but if we don't come to agreement, the Federal Government has the ability to unilaterally impose a change on this allocation.

Ms. DEGETTE. Thank you.

Mr. STUPAK. Mr. Burgess.

Mr. BURGESS. Thank you, Mr. Chairman.

Mr. D'Agostino, just so I'm clear on this, I think Deputy Secretary Sell testified that you were the selector in the RFP process a little over a year ago; is that correct?

Mr. D'AGOSTINO. Yes sir, that is correct.

Mr. BURGESS. You mentioned in your testimony about recompeting the contract. I'm assuming there you were talking about the recompeting of the contract that happened a year ago, not a recompete that's at some point in the future.

Mr. D'AGOSTINO. I'm actually referring to a recompete if it should come to this point. If it should come to the point where myself as the Acting Administrator of the NNSA feels that we have a material breach of the contract or we have a situation where it's in the best interest of the Government, I, as the Administrator, through my contracting officer, have an ability to recompete.

That is not the case right now. I want to make that clear because I do believe we don't have—we don't have all of the analysis together as a result of the current criminal investigation that's underway.

Mr. BURGESS. But you do have the ability, then, to recompete the contract.

Mr. D'AGOSTINO. The contract allows me to terminate for cause of the existing contract.

Mr. BURGESS. Without waiting the 7 years to do so?

Mr. D'AGOSTINO. That's right. Yes, sir.

Mr. BURGESS. Well, let me just ask you a question then.

We've heard all kinds of testimony about the fines levied, whether it's $3 million or $73 million; and $73 million would be a significant fine to levy against the contractor.

Would they be able to continue in their mission if they were hit with that level of fine? Would that damage their ability to provide the services, the security that we're going to demand of them?

Mr. D'AGOSTINO. I believe that if I were to decide today that I wanted to levy, and I had all of the data with me today that it would be a bad management decision to make that move right now before the fiscal year is over. I have complete faith and confidence in Dr. Anastasio. I understand the plans he's putting in place. He does take this seriously. He has taken specific steps. There are obligations on the part of the Federal Government as well, and I'm making changes on that particular side. But I do believe that it would be irresponsible and a bad management move from my years of managing organizations, before the fiscal year is actually over, to make that decision.

So, to answer your question, I wouldn't do it at this point, but what's clear is the fee is an amount of resources that are set aside.

Mr. BURGESS. Well, let me just interrupt you then.

As far as just the management aspects of it, we had a team that was on site for over 60 years. I'm relatively new, but it sounds like, on this committee, we've been dealing with the same sort of problem over and over again. I don't know whether they're interrelated or not. I've got to assume that a laser injury of the eye is not related to the removal of a thumb drive, is not related to the guy getting beat up at the bar, but still there are all these things that keep coming up.

How good a management decision is it to continue on with the same group that has brought you these troubles in the past, and should we not have been able to anticipate a subsequent breach because of the behavior that at least has been exhibited since 1999?

Mr. D'AGOSTINO. Sir, I'd like to address that in two ways. One is to make sure that it's clear that the same organization is not running this laboratory. It's clear that the proposal that I reviewed——

Mr. BURGESS. Has the culture actually changed then since the awarding of the contract?

Mr. D'AGOSTINO. I would say I don't know the answer to that question, but here's what I will——

Mr. BURGESS. I hope you find out quickly.

Mr. D'AGOSTINO. That's exactly right.

The LANS executive committee knows. The Executive Board of Governors, the executive committee on the board, truly understands, because I put this in writing, that I don't believe this is just a matter of, well, let's straighten out our policies and procedures, do a couple of checks and follow up, and everything will be all right.

My job as a manager is to set expectations, to man performance and then follow up and use the tools that I have. This structure actually allows me the opportunity to do that. Never before has the Department had this much money on a contract.

Mr. BURGESS. And I hope you have the courage to enforce that.

Ms. Wilbanks, let me just ask you briefly. You used the word "malicious" in your testimony. Did I understand that accurately?

Ms. WILBANKS. Yes, sir.

Mr. BURGESS. So this person willfully downloaded material, took it back to her living quarters. What would be the—if I'm going to do something maliciously, presumably I have a reason for doing it. Have you explored that? Do we know what that answer is or is that still locked up in the FBI report?

Ms. WILBANKS. I believe it's part of the FBI investigation, sir.

Mr. BURGESS. And at some point, again, Mr. Chairman, that information is going to be shared with us?

Mr. ANASTASIO. Mr. Chairman, Congressman, if I could try to answer that briefly, in all the conversations that I've had with the FBI, they've given me no evidence that anything's happened beyond taking that material to her home.

Mr. BURGESS. But there must have been some financial incentive or wanting to damage someone. I mean you don't just do something like that on a whim, or at least I can't believe that you would.

Mr. ANASTASIO. Certainly, the FBI is the one that can answer that in better detail, but what they've expressed to me in my variety of discussions with them is they have no indication that she did anything beyond what was reported in the press.

Mr. BURGESS. But, again, the motive—I mean the laser injury to the eye, OK, that was an accident; getting beat up in a bar, that's bad judgment; but taking material from the server back to your living quarters—I mean there's got to be a reason why someone would engage in that type of activity. It was either for sale or to damage someone else. But again, we don't know the answer to that at this point.

Mr. ANASTASIO. But what we are working hard to do is make sure that never happens again.

Mr. BURGESS. And I would very much like an answer as to why it happened in the first place.

Do we get another round?

Mr. STUPAK. We'll just do one more question or so.

To get back to the FBI, we talked a little bit off the record there. We'll try to have them come in and give us a briefing, a members' briefing, on the status there to answer some of your questions.

Mr. Melancon.

Mr. MELANCON. Thank you, Mr. Chairman.

Mr. Anastasio, you talked earlier about disciplining about 20-some-odd people. What were the violations that you disciplined them for?

Mr. ANASTASIO. We did a very extensive review with a detailed look at all the incidents going back to over a year and a half ago when this project was first set up. The conditions of security that were built into the planning that they did, all the way through the activities, up until—up until the recent times, and in that, there were a variety of people that were disciplined, either removed from their job or other forms of discipline for all of the different sorts of things that went on, which were bad judgment on the part of employees, bad policies and procedures that were in place and things of that nature.

Mr. MELANCON. Can you give me an illustration of what, maybe, the worst one was or one of the worst ones?

Mr. ANASTASIO. I think the worst problem was the way the security was set up for this particular project. The people who set it up actually were trying hard to be very conscious of security, but they didn't—they didn't make a plan that addressed all of the potential risks, and the people that were responsible for that security plan in that vault-type room, I think, were the ones that got the most severe penalty. And then the second-most, I would say, was the—was the cybersecurity team that was responsible for the overall policies of the institution.

Mr. MELANCON. Of the 20-some-odd, how many did you fire?

Mr. ANASTASIO. Three were removed from their assignments. Many of the people who were responsible for this activity were no longer in the same assignment when we came on board, so they had been moved out of their job for a variety of reasons before we even got there, even though they were responsible a year and a half ago for—for overall security things.

Mr. MELANCON. Have you been—I don't know if you've been there shortly, but has the process been to try and ferret out all of these people from as far back—of course, I don't know how far back you go.

Mr. ANASTASIO. Yes, we went back to the very beginning when the project was set up. We identified all the people who were responsible. The organization itself that was responsible at the time doesn't any longer exist. We've reorganized, et cetera, but we went and identified all of the individuals who have been involved over this entire period of time and, again, went through a very detailed effort to examine all the issues and who was responsible for them, and that led to the 24 different disciplinary actions.

Mr. MELANCON. You ran Lawrence Livermore; is that correct?

Mr. ANASTASIO. Yes, sir.

Mr. MELANCON. How many employees are there at Lawrence Livermore?

Mr. ANASTASIO. Oh, I guess I don't remember offhand. I'd say about 8,000 to 9,000.

Mr. MELANCON. So about two-thirds to three-quarters of what you have at——

Mr. ANASTASIO. That's approximately right.

Mr. MELANCON. Yes, and there's not any security problems that you experienced there, cyber or otherwise?

Mr. ANASTASIO. There were some security problems at Lawrence Livermore while I was there. One incident that got quite a lot of attention was some security keys that got lost. And the approach I'm taking to the incidence here is the same I took there, which is to act very quickly and decisively, to find out those who were responsible and make sure that they're properly held accountable, and to go build a system that addresses the issues. And I would say—I'd defer to others, but I've been told that Lawrence Livermore now has the model security program for keys in the complex, and in fact, the lab goes around and briefs the other sites on the lessons learned and how to do a better job. So I think we responded very decisively there, and that's been my intent to do here at Los Alamos.

Mr. MELANCON. Yes. I guess the thing that I'm having problems getting my arms around is that this country—of course, I guess, when you look at Homeland Security, maybe we really do have a problem, but it's not at your level. But when you look at the security that is provided in this country and other places by our Government, why is there not some type of guideline, some type of program that we can model after? I mean this is—are we making it up as we go when we brought these new contractors in?

Mr. ANASTASIO. Well, certainly, there's an element that's very clear on how to do this that has the behavioral issues involved, that has issues of policies and procedures, infrastructure that we've talked about, how big is your infrastructure, et cetera. But there's another piece which I think is a very large challenge for the country and us at the laboratory, which is the advance of technology.

The last time the laboratory reviewed its policies—and we could argue they should have done it much sooner—these little memory stick, thumb drives were not in common usage, and yet now that they are, it's quite obvious what a risk they are for security. And so what's going to be the challenge we have 2 years from now is we really need to develop a system in place that's robust against the future advancement of technology so we don't have to fix it after the fact like we're doing now. And that's the plan we're off doing.

Now, I would argue that, as one of the previous witnesses has testified, there are a lot of nefarious people out there who are very sophisticated who are always looking to get access, and that also concerns me very much. And finding a way to defend ourselves from those kinds of attacks as well as the kind we're talking about here is a deep concern to me.

Mr. MELANCON. Thank you, sir.

My time has expired.

Mr. STUPAK. We'll move quickly and see if any members have further follow-up. There's been some expression of wanting to follow up. If I may, just two questions.

Mr. Anastasio, you indicated the thumb drives—when that cybersecurity was done, thumb drives weren't in use, but if you'll look after January 2005, after they shut down the lab for a while, five out of 14 points dealt with cybersecurity, dealt with the fact that these things are accessible. So I would suggest that maybe a good place to start for security is go back and look—after we shut down the lab that cost $350 million, that we look at the recommendations that were made and implement those procedures.

Mr. ANASTASIO. I can't speak to exactly what happened during—during that shutdown and why they did it.

I can say that we have looked at and have, in fact, developed plans for all the issues that came up associated with that shutdown, and the corrective actions in place. We have a very effective system in place now to keep track of those about who's responsible to——

Mr. STUPAK. Sure, but in Mr. Melancon's answer, you said the last time you had a security review like that, thumb drives weren't being used. They were certainly in use in 2005 and long before that.

Mr. ANASTASIO. Yes, sir, and I guess what I was—maybe to be clearer, the policies that the laboratory has for cybersecurity were not changed to be cognizant of the new technology that was available, and that was a mistake on the laboratory's part, and we're all fixing that.

Mr. STUPAK. Ms. Wilbanks, I was asking you some questions about the cybersecurity and the computer systems, and I'll ask you the same thing. Had you reviewed the 2004—or after the 2004 report—recommendations made, and you indicated that there wasn't much in there about cybersecurity, but yet five of the 14 recommendations deal with cybersecurity. In fact, as you are the Chief Information Officer, it even states—and I'm looking at the January 2005 memo. It says that the Office of Chief Information Officer is leading the effort to implement a cybersecurity enhancement plan to protect the confidentiality, integrity and availability of all DOE information systems.

So you certainly, as the Chief Information Officer, have a huge role to play in shoring up all the classified and unclassified systems, including cyber; is that correct?

Ms. WILBANKS. Yes, sir.

Mr. STUPAK. OK, and with that, Mr. Whitfield.

Mr. WHITFIELD. Thank you, Mr. Chairman.

Just a couple more questions.

Mr. Anastasio, what is—do you have a policy on whistleblowers?

Mr. ANASTASIO. Yes, sir, we do.

Mr. WHITFIELD. OK, and I'm assuming you encourage——

Mr. ANASTASIO. Absolutely. And we have a number of mechanisms in place to allow anybody at the laboratory who has a concern that they feel they can't discuss with their line management, they had, as a confidentiality process, a separate group of people to—to—we also have an ombudsman program. We have a variety of mechanisms that employees have available to them.

Mr. WHITFIELD. OK, and then as a result of the deputy lab director announcing his retirement, which basically was in violation of the contract, the contract administrator or contracting officer,

Edwin Wilmot, wrote a letter to you on December 6, requesting a briefing on what steps you all intended to take to ensure the retention of all key personnel.

Now, have you all had that briefing yet or——

Mr. ANASTASIO. I have not formally responded to his letter, but he and I, in fact, just last week talked about this very subject on the phone, and I gave him an update, and he requested me to send him some more information which I promised to do right after this hearing.

Mr. WHITFIELD. OK. And then just one other comment. Ms. DeGette's questions made me think of this a little bit.

The base contract, Mr. D'Agostino, is $1.5 billion to $2 billion; is that correct, roughly?

Mr. D'AGOSTINO. It's roughly $2 billion, sir.

Mr. WHITFIELD. And that's basically for managing the site?

Mr. D'AGOSTINO. That's right. It's for managing the site. There's a fee element associated with that. That's right.

Mr. WHITFIELD. And then, on top of that, we have a $73 million pool that can be given for extraordinary performance or incentives or whatever; is that correct?

Mr. D'AGOSTINO. As a subset, sir, not on top. It's roughly $2 billion. It depends on how much work we allocate to Los Alamos National Laboratory and the amount of work they have. The laboratory gets its resources from a number of different areas within the Department and across the Federal Government. About 60 percent of it, maybe closer to 70 percent of it, actually comes from the NNSA. Probably about 15 percent of it comes from other elements of the Department of Energy, and about 15 percent comes from what we call "work for others," which is work for other Federal agencies, the Department of Defense and other intelligence agencies.

Mr. WHITFIELD. But the $1.5 billion to $2 billion, that actually is paid to the M&O contract holder?

Mr. D'AGOSTINO. Right. That's the sum total of that text that I just described to you earlier, and the fee element is essentially an indirect charge that we allow the laboratory and part of its management to make it an allowable cost, and it's set aside in a specific account within the indirect pool, so it's not in addition to on top of, sir.

Mr. WHITFIELD. OK.

Mr. ANASTASIO. Excuse me, Congressman, but that $2 billion is to execute work. That's well——

Mr. WHITFIELD. OK.

Mr. ANASTASIO. That's well defined by Congress and by the Department that here's a set of work activities for us to go and do.

Mr. WHITFIELD. OK. Thank you.

Mr. STUPAK. Ms. DeGette, any follow-up?

Ms. DEGETTE. Ms. Wilbanks, when I was at the facility in 2004, we were told that all of these ports were going to be secured then. And then in your testimony today, you said that since this incident, you've secured all USB ports at all NNSA sites and are reviewing all cybersecurity plans to ensure that they address the specific risks for the system. This type of incident, the undetected transfer

of classified information to a portable device, could no longer occur at any NNSA site.

I guess my great frustration here and, I think, the frustration of the rest of the committee is that we keep trying to close the barn door after the horse escapes. Mr. Anastasio says, well, now we're drug testing the employees before they get through the security system. Now you're in here saying that the ports have been secured.

Why didn't that happen before this incident? If we knew the problem existed several years ago, why didn't it happen?

Ms. WILBANKS. I did not come to the Department of Energy until the end of October 2004, so I can't speak to the comment that was made before I was there.

I can tell you that the ports have been in the process of being closed, and the sites have been working on it. I don't have any other——

Ms. DEGETTE. It took 2½ years to do that?

Ms. WILBANKS. I don't know, ma'am.

Ms. DEGETTE. OK. When did you say you came?

Ms. WILBANKS. October 31st, 2004.

Ms. DEGETTE. OK. So that was right after we were there, and so when you came, and then in October of this year, that was 2 years, and the ports still weren't closed in that time, right?

Ms. WILBANKS. Yes, ma'am. There was no policy or procedure in place to require the port closure. It was not identified as a high risk is my assumption.

Ms. DEGETTE. OK. So, if we were told—you would have no knowledge—so no one told you that that was a high priority?

Ms. WILBANKS. No, ma'am. I was not aware of it.

Ms. DEGETTE. OK. See, that's why we're so frustrated is because, when we were there earlier that year, we were told that that was a high priority.

I guess this is what you're talking about, Mr. Anastasio, about the unclear competing policies.

Thanks. This is what they secure it with, this JB Weld.

Ms. WILBANKS. Yes, ma'am.

Ms. DEGETTE. So how would that take 2 years? Because it wasn't a high priority, I guess.

Ms. WILBANKS. That would be my answer, ma'am.

Ms. DEGETTE. I'll yield to you, Mr. Stupak, for the JB Weld question.

Mr. STUPAK. Thanks for yielding.

I mean, wouldn't you anticipate—if you're security experts, wouldn't you anticipate that someone's going to take a thumb drive and put it in these computers?

Ms. WILBANKS. No, sir. She was in a classified environment that only cleared——

Mr. STUPAK. No. No. No. I'm not saying this lady.

You've got 25,000 computers out there that you say contain sensitive information. If anyone can just take a thumb drive—and I think Mr. Friedman held it up earlier and said you could take two file cabinets full of information off of it—wouldn't you so-called "security experts" think of that? I mean someone thought of it in 04 and told us when we were out there. That's the part that's baffling.

I yield back.

Ms. DEGETTE. I just think, Mr. Anastasio, that you really have a job ahead of you, and I hope that you and your team can do that job because I don't think there's very long for that to happen before we do take really drastic changes. We've been sitting here for 8 years doing this, and this is a perfect—drug testing is another example. I'm assuming at Lawrence Livermore and at other labs that drug testing for high-level security clearances is pro forma, wouldn't it be?

Mr. ANASTASIO. There was not a policy for drug testing at Lawrence Livermore when I was there. We have a requirement for certain specific activities, the handling of nuclear material, for example, that the Department requires us to have a drug testing program for, and of course those are in place all across all the sites.

What I've done at Los Alamos is to say that, actually, I'm going to have drug testing for all employees whether they have a top-level security clearance or not.

Ms. DEGETTE. And just——

Mr. ANASTASIO. For anybody who comes to work at my site, I won't stand for people using illegal drugs.

Ms. DEGETTE. Well, that's good. But even under the previous standards, this gal who was cleared probably shouldn't have had that level of security clearance, wouldn't you agree?

Mr. ANASTASIO. I can't speak to that. I don't know. I don't know all the background that she had and that led to her—the decision about the clearance.

Ms. DEGETTE. Thank you.

Thank you. I yield back.

Mr. STUPAK. Mr. Burgess.

Mr. BURGESS. Thank you. And Mr. Anastasio, it just seems incredible that we will drug test our athletes. In fact, we've had hearings in this very room about that. We'll drug test our athletes, and we're not drug testing at Lawrence Livermore. I don't see that as good information.

Mr. Pyke, let me ask you a question.

The designation of an "official use only" document, what would be the reason to designate something as "official use only"? Would that mean that we shouldn't be distributing it, say, around in this room for everyone to look at?

Mr. PYKE. My understanding is that the "official use only" designation is given when someone has reason to believe there's sensitive information in there that should not be disseminated broadly.

Mr. BURGESS. Then, of course, you're aware that one of our staff members this morning downloaded a document from your Web site that's marked "official use only".

Mr. PYKE. His report to me, late morning, is very disturbing to me, and in fact, I would appreciate it very much—he reported something similar last year, and I'm told that our staff went out and assured that the offending material had been taken down immediately, that very day, off of the Web. I gave directions right after I heard from him this morning that if, in fact, that information is still on the Web, that it be taken down immediately.

We have a clear directive to the Department that not only is OUO and other sensitive, unclassified information not to be placed on the Web, to say nothing of classified information not to be placed on the Web, but there is to be a process in place to ensure regular monitoring of Web sites to ensure that such information has not crept onto the Web by mistake or otherwise.

Mr. BURGESS. Or otherwise. With all of the talk that we've had this morning, you do have to worry about the "otherwise". Fortunately for you, I'm not smart enough to understand what I'm holding in front of me. I don't know that I can say the same about the staff member who downloaded it, and if it's not off the Web site, I do encourage that you do that.

Just as a final thought on everything we've been talking about this morning, I hope we don't focus on so much the individual worker at Los Alamos, the person who may have given in to a moment of human frailty, but we really have to put those procedures and the culture in place that just does not allow this to happen in the future. And heaven help us all if we're back here doing this same thing in 6 months' time.

I yield back, Mr. Chairman.

Mr. STUPAK. OK. Our witnesses, nothing else?

OK. Well, thank you and you're excused.

We will go into executive session in 2218, Room 2218, in 15 minutes, 2:05, Mr. Friedman, Mr. Podonsky and Deputy Secretary Sell, if you would, please.

This record will remain open for 30 days. If members have questions they'd like to submit to any of the witnesses, that record will remain open for 30 days for those questions.

[Whereupon, at 1:51 p.m., the subcommittee proceeded in executive session in room 2218.]

[Material submitted for inclusion in the record follows:]

**Introduction**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**LANS Approach to Enhanced Security**

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

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

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

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

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

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

**Are We Really Different?**

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

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

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

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

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

**Summary of the Incident**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Disabling Classified Computer Ports*

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

*Suspended Classified Scanning Activities*

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

*Review Subcontractor Security*

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

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

*Security Escorts*

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

*Employee Training and Communications*

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

*New Cyber Security Organization*

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

*Increased Physical Searches*

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

*Enhanced Drug Testing Policy*

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

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

## Accountability

*Termination of Subcontractor Contracts*

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

*Employee Disciplinary Actions*

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

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

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

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

**LANS Commitment**

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

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

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

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

**Solution and Path Forward**

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

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

*Clear Lines of Management Authority*

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

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

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

*Continue the Walk*

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

*Interim Cyber-Security Organization*

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

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

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

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

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

*Compliance with Recent DOE Cyber Security Guidance*

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

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

*Outside Cyber Security Experts*

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

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

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

*Vault Type Room (VTR) Security Pilot*

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

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

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

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

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

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

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

*Performance Based Leadership*

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

*Other Initiatives*

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

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

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

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

## Conclusion

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

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

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

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

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

Thank you.

ANSWERS TO SUBMITTED QUESTIONS

**Please identify exactly how many classified computers there are at Los Alamos National Laboratory (LANL). Please also describe in how many different locations these computers reside, and how many computers have open Universal Serial Bus (USB) or firewire ports. Please describe why each computer is essential and whether there are opportunities to reduce and consolidate the number of classified computers.**

The Los Alamos National Laboratory occupies 43 separate technical areas spread across an approximate 40-square-mile site. When Director Anastasio testified in January, we reported an inventory of 3,310 classified systems, 2,990 (89 percent) of which were networked and 320 (11percent) were non-networked. Of the networked systems, 430 were servers and 2,560 were user systems. The non-networked systems consisted of 240 desktop systems and 80 laptop systems. Non-networked systems are generally utilized in areas where classified network connections are not available or to address information protection requirements. Laptop systems are needed for experiments conducted in remote regions of the LANL site and to which data acquisition equipment must often be transported, and also are an essential component for nuclear emergency response activities. When not in use, the non-networked laptop systems are protected as accountable CREM by storing them in a classified media library.

As of the time of this response, LANL has 2,912 classified systems, of which 2,653 (91 percent) are networked computers and 259 (9 percent) are non-networked. Of the networked systems, 450 are servers, and 2,203 are user systems. The non-networked systems include 54 laptops, 198 desktops, and seven custom experimental devices. The reduction is due both to conscious decisions made to reduce the total number of systems (for instance 94 non-networked systems were decommissioned in the first quarter of this year) and changes in our programmatic activities and their associated needs for classified computing.

Only seven of Los Alamos's 43 technical areas house classified networked computers. Sixty percent of our networked classified computers are located in a single technical area. Twenty-seven percent are located in two other technical areas and the remaining systems are found at four other technical areas. Non-networked systems are found at 14 technical areas; 50 percent at a single technical area, seven percent at another technical area, and the remaining systems are scattered between the other 12 technical areas. Nine of the 14 technical areas do not house any networked computers. Twelve classified media libraries currently store the non-networked classified laptops when they are not in use.

All classified computing is performed in security areas.

As with the above reductions made in the number of classified systems, LANL has also made major changes in the control of USB and firewire ports since the time of the incident last Fall. Currently, there are no ″open″ USB or firewire ports on classified systems (with the exception of systems used by the nuclear emergency response teams, which constitute a very small percentage of Los Alamos' total classified computing resources). All USB and firewire ports have been protected by one or more methods that have been approved by the NNSA Los Alamos Site Office.

The number of computers at LANL varies with changes in our programmatic efforts. Expenditures for classified computers, as with other equipment, are appropriately justified based on programmatic need. Specific discussion about why each program requires the specific computers supporting it would render this response classified. In general, the classified computers at LANL support the following areas:

- Nuclear weapons design
- Stockpile stewardship
- Pit production
- Homeland security and threat reduction
- Nuclear emergency response
- Intelligence community support

LANL is taking a number of actions to further reduce risks. For instance, LANL is emphasizing standardizing the types of systems used, networking as many of those as possible to permit consistent system administration, reducing accountable CREM, monitoring computer activity, and consolidating locations where such services as classified printing, media generation, and matter storage are available to improve the control of system output mechanisms. As an example, the Super VTR prototype is expected to eliminate at least six other vault-type rooms and five classified media libraries.

**Please identify exactly how many classified security areas there are at LANL. Please describe why each classified security area is essential and**

**whether there are opportunities to reduce and consolidate the number of classified security areas.**

Currently there are 1,372 distinct and separate buildings where classified activities occur and where the appropriate levels of security are provided. These 1,372 buildings are located within 108 "Security Areas," each enclosed by security fences and access gates. Each building/area where a classified activity occurs has a unique significance relative to national security that is mission-specific to those locations. The majority of these buildings contain classified repositories that reduce the necessity and frequency (and resultant risk) of transporting classified documents/materials between locations.

We are continuing our comprehensive review of locations and holdings to ensure this number is reduced to the absolute minimum consistent with operational requirements.

**Please identify exactly how many classified vaults there are at LANL. Please describe why each classified vault is essential and whether there are opportunities to reduce and consolidate the number of classified vaults.**

There are currently 129 Vaults and Vault Type Rooms at LANL. Of that, 11 of those facilities are true vaults. Each Vault or Vault Type Room has a unique significance relative to national security that is mission-specific to the location. Since October 1, 2006 LANL has embarked on a continuing process to consolidate and reduce the number of these types of facilities. Since then, LANL has successfully reduced the number of Vaults and Vault Type Rooms from 142 to 129 using the following criteria:

- Wherever possible and when programmatic compartmentalization responsibilities allow, remove classified material and consolidate into existing Vaults and Vault Type Rooms.
- In cases where aging infrastructure make compliance with physical security standards and maintenance of intrusion detection systems cost prohibitive, classified assets are to be consolidated into newer, compliant Vaults and Vault Type Rooms.
- Those existing Vaults and Vault Type Rooms that only house classified computing infrastructure like server racks and networking systems hardware are to be given a priority for review for consolidation and reduction.
- LANS is piloting a Super Vault Type Room project where similar classified processing activities are to be consolidated into a single facility. The first Super VTR will combine at least six Vault Type Rooms into one. As funding becomes available for additional Super VTRs, additional consolidation will be possible.

These efforts are ongoing and should lead to future further reductions in the number of Vaults and Vault Type Rooms at LANL. To put our efforts in context with the DOE complex, Lawrence Livermore National Laboratory, Sandia National Laboratory and the Pantex Plant currently manage over 200 Vaults and Vault Type Rooms each.

Testimony of
Danielle Brian, Executive Director
Project On Government Oversight (POGO)
before the
House Energy and Commerce Committee's
Subcommittee on Oversight and Investigations

"Continuing Security Concerns at the Los Alamos National Laboratory"

January 30, 2007

Thank you for inviting me to testify today. I am Danielle Brian, Executive Director of the Project On Government Oversight (POGO), an independent nonprofit that investigates and exposes corruption and other misconduct in order to achieve a more accountable federal government. We have been investigating and exposing security failures in the nuclear weapons complex since 2001 and have issued three reports on the topic so far: *The U.S. Nuclear Weapons Complex: Security at Risk* in 2001, *The U.S. Nuclear Weapons Complex: Homeland Security Opportunities* in 2005, and *The U.S. Nuclear Weapons Complex: Y-12 and Oak Ridge National Laboratory at High Risk* in 2006.

After the Wen Ho Lee debacle of the late 1990s, a brand new, semi-autonomous National Nuclear Security Administration (NNSA) was created to improve security – and in particular cyber-security – in the nuclear weapons complex. Despite the creation of this agency, security failures continued to plague the complex. Of primary concern has been the Los Alamos National Laboratory. Many people, including those of us at POGO, believed the consistently poor performance in security at the Lab was because the same contractor, the University of California (UC), had been running Los Alamos for 60 years without fear of losing its contract – no matter how badly it ran the Lab. There was no incentive to do things well. Finally, after much pressure

666 11th Street, NW, Suite 900 • Washington, DC 20001-4542 • (202) 347-1122
Fax: (202) 347-1116 • E-mail: pogo@pogo.org • www.pogo.org
POGO is a 501(c)3 organization

from this Committee and others, then-Energy Secretary Spencer Abraham announced that he would compete the contract. On December 21, 2005, Secretary Samuel Bodman announced that the UC / Bechtel team had won the contract to run the Los Alamos Lab. At the time, many doubted that this team was anything more than the same old UC in new clothing. However, Secretary Bodman stated:

> I cannot stress enough . . . that this is a new contract, with a new team, marking a new approach to management at Los Alamos. It is not a continuation of the previous contract. That is how our Department views the situation from this point forward. . . . There has been quite a bit of turmoil and uncertainty over the last few years. Today's announcement is designed to relegate that tumult to the past, and to usher in a new era of invaluable, cutting-edge science at Los Alamos. So this is a good decision for the men and women who make up this lab. And let me take this opportunity to mention that this evening, Ambassador Brooks will be flying to New Mexico.

Yet, here we are just over one year later and Ambassador Linton Brooks has been asked to resign; our nation's secrets have been mishandled by Los Alamos – again; and the suspicions of many were fulfilled: Nothing has really changed at Los Alamos after all. In fact, I fear things may actually be getting worse. Not only has NNSA has failed to correct security issues, but the agency has determined that it wants even <u>less</u> oversight of Los Alamos and has implemented a new pilot program in which oversight has been handed over to the contractor itself.

Since 2001, when POGO began investigating the security of the Nuclear Weapons Complex, there have been at least seven instances in which classified information was mishandled at Los Alamos. Classified computer disks have gone missing; computers that may have contained classified information somehow disappeared from Lab property, either having been stolen or lost; classified information has been transmitted through unsecured emails; and the list goes on. A cyber-security episode has occurred, on average, nearly once a year since POGO began its investigation. And all these instances occurred after the infamous episode of the two missing hard drives, which contained highly classified, Sigma-14 Nuclear Emergency Search

Team (NEST) data and which were later discovered with all the fingerprints wiped away behind a Xerox machine.

Now, in the most recent incident, a subcontractor employee freely took over 200 pages of hard-copy classified documents and over 400 classified documents on flash drives to her home, which she shared with a drug dealer.[1] This could only have happened if there was a complete collapse of multiple supervisory and security systems. It was only by happenstance that she was caught, not because an effective security system was in place. We never would have known about this security breach if it hadn't been for a domestic disturbance. Furthermore, we have no way of knowing how many other instances like this are out there but have flown below the radar. It is important to remember that NNSA attempted to keep this incident secret from Congress and the public, until POGO learned about it eight days after a local police raid.

As a side-note, if media reports and statements by investigators are accurate, this most recent case points to extraordinary failures in the personnel security clearance process, in addition to cyber-security failures at the Lab. However, given that this case is still under investigation, we don't believe it is appropriate to discuss the security clearance process in a public session. Furthermore, it is only since this incident that Lab management is recommending that Los Alamos employees be subjected to drug testing, which I understand is very controversial at the Lab. How could it have taken so long to take such a basic step? Even my 16 year-old son had to take a drug test to work at Target, where he straightens up the ketchup bottles.

After the most recent security incident at the Lab, a cyber-security audit was launched. According to a Lab email, which I would like to submit for the record, "As a result of the preliminary findings of [the Cyber Security] audit, LANL has agreed to suspend all non-essential

---

[1] "Nuclear lab's security scrutinized," CNN, October 26 2006, http://www.cnn.com/2006/US/10/26/los.alamos/index.html ; "Drug Raid Yields Los Alamos Documents," by Lara Jakes Jordan, Associated Press Writer, October 25, 2006, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2006/10/24/national/w162852D72.DTL ; "New Details Emerge In Los Alamos Case: Top Nuke Lab Data Leak Apparently Discovered During Drug Bust; Officials Search For Ties," CBS News, October 25, 2006, http://www.cbsnews.com/stories/2006/10/24/national/main2122004.shtml.

classified computing activities for a least the next 48 hours by the close of business today." This is not the first time security failures have significantly impacted operations at the Lab.

In 2000, shortly before leaving office, then-Secretary Bill Richardson announced the complex was going "media-less" or "disk-less," so that there would no longer be Classified Removable Electronic Media (CREM) to be lost or stolen. The labs ignored the order. In May 2004, then-Secretary Abraham announced that the complex was going to a disk-less system. Again, the labs ignored the order. Then, two months later after yet another mishandling of classified media, Abraham shut down all classified operations at Los Alamos for over eight months. This closure cascaded around the complex and, in total, cost the taxpayer over $500 million because the contractor continued to get paid while little or no work was accomplished over those months. UC was not penalized for this, and it is unclear what, if any, costs were disallowed during this period. Instead, UC was re-awarded the contract. And after all that time and money, flash drives are being discovered in trailer park meth labs.

I suspect Secretary Bodman will soon be announcing a new initiative to solve cyber-security problems, and I am sure he is genuine in his belief that his directives will fix the problem. But those of us who have been around for a while have reason to be skeptical.

CYBER-SECURITY IS NOT THE ONLY PROBLEM AT LOS ALAMOS

In addition to cyber-security failures, Los Alamos continues to suffer from safety problems. Recent safety incidents include: a post-doctoral student was shot in the eye with a laser; two workers were forced to work in an area where acid was burning their lungs; a hose came loose in a glove box at TA-55, seriously contaminating several workers with highly carcinogenic plutonium; a worker was contaminated with americium, and went on to contaminate houses and cars in four states costing over one million dollars to clean up; and the plutonium facility was forced to shut down for over a month when it was discovered that the sprinkler heads in the fire suppression system had been non-functional for years because they had been painted over, costing $6 million to replace them. At the time, DOE also discovered that the

contractor, the University of California, had never tested the fire hoses in the plutonium facility. Despite these and other examples that demonstrate how the Lab minimizes the value of safety and security requirements, NNSA has rewarded the Lab with decreased supervision through the self-policing pilot program.

In addition to mishandling our country's nuclear secrets and repeated safety violations, Los Alamos has also been the home of a litany of corruption and misconduct. Many of you were on the subcommittee that heard the testimony of two top security officials at Los Alamos, Glenn Walp and Steve Doran. They described uncovering crimes ranging from petty theft to organized fraud, and the Lab's active efforts to conceal this misconduct. As thanks for their good work, Walp and Doran were fired and escorted off the property by armed guards. As you may recall, a number of Lab officials were fired over misconduct surrounding the Walp and Doran revelations, and others were sent to prison. What you may not know is that after the furor died down, a number of those individuals were either re-hired or given huge payouts from the Lab. This is clear evidence of a culture that punishes those who raise concerns and protects those who "protect" the Lab from scrutiny.

Auditors at Los Alamos also continue to come to POGO with serious concerns about the auditing and investigations functions at the Lab: Because these functions have been so pared down, and because the contractor has the ability to control and limit access to cost and pricing data, there are no honest, independent reviews to determine how the $2.2 billion that taxpayers give to Los Alamos annually is spent. In December 2005, the DOE Inspector General supported the claims of whistleblowers, stating their allegations "had merit because our results were similar and Los Alamos officials acknowledged that internal control weaknesses existed . . . ."[2] Yet, rather than being rewarded for their diligence, the whistleblowers were given no work for years and treated as though they themselves were the problem.

---

[2] *Assessment of Changes to the Internal Control Structure and their Impact on the Allowability of Costs Claimed by and Reimbursed to Los Alamos National Laboratory under Department of Energy Contract No. W-7405-ENG-36.* Audit Report Number: OAS-V-06-07. U.S. Department of Energy Office of the Inspector General. December 23, 2005.

LOS ALAMOS IS NOT THE ONLY PROBLEM IN THE COMPLEX

It is important to remember that Los Alamos is a big problem, but also that it is not the only problem in the nuclear weapons complex. Senator Chuck Grassley (R-IA) has been performing aggressive oversight of security failures at the Sandia National Lab for several years, but those failures are beginning to raise their ugly heads again. Alarms are allegedly being turned off – apparently to make it easier for guards to sleep. At Pantex, where hundreds of nuclear weapons are stored and dismantled, significant safety breakdowns have been identified by the Defense Nuclear Facilities Safety Board, yet DOE has done little to address these concerns. NNSA has imposed two fines for safety, the higher for almost $124,000, but this is a slap on the wrist for the contractor given the $30 million award fee. At Los Alamos and Y-12, where over 400 tons of highly enriched uranium are stored, DOE has waived until 2011 the requirement that the sites meet security standards (the Design Basis Threat).

And at the moment, the contract to operate Lawrence Livermore Lab is up for competition. It appears, however, that this competition may be in name only: The same contractor that currently operates Livermore – UC – is poised to get the contract again. In 2006, then-House Appropriations Subcommittee on Energy and Water Chairman David Hobson wrote of his concerns, and I ask that the entire letter be entered into the record:

> I am very disappointed with the results of the contract competitions that the Department has conducted to date. . . . I have had potential competitors inform me that their companies will not invest the time, effort, and expense to prepare a proposal for the Livermore contract because they believe that the Department is determined to award the Livermore contract to the University of California. . . . In mandating competition, it was the intent of Congress to attract the widest possible group of interested bidders to bring in fresh ideas and new talent to support the Department's mission. Unfortunately, the Department of Energy's national laboratories are not viewed as a competitive marketplace but as a playground for political patronage. The Department of Energy has resisted moving in the direction of fair and open competitive processes. Unfortunately, the Department has insisted on using the flawed Los Alamos competition as a model for the competition for the Livermore contract, which telegraphed to the contractor community that innovative ideas and concepts would not be favorably received. . . . We need a procurement process that fosters greater competition, not a process that essentially guarantees the status quo.

LOS ALAMOS AS THE BAD CHILD

Despite these other sites that also urgently need addressing, Los Alamos sticks out as the bad child. Why?

There is a joke around the complex that goes something like this: The Secretary of Energy tells the three national labs to jump. Sandia asks how high, Livermore makes an excuse for why it's too busy to jump, and Los Alamos asks who the Secretary of Energy is. Los Alamos sticks out as the bad child because of its consistent and utter disregard for federal oversight.

At this rate, we can all schedule next year's hearing right now, given the likelihood that we'll still be discussing problems at Los Alamos unless the entire incentive system is reversed.

RECOMMENDATIONS

Secretary Bodman sent a strong message earlier this month when he asked NNSA Administrator Brooks to step down. He made it clear he was serious and wanted change. But getting a new Administrator is not enough: There needs to be an upheaval in the current system of incentives.

First, there needs to be a renewed commitment to independent federal oversight from the Department of Energy. In its current state, the Site Office is non-functional. There are apparently over twenty vacant federal positions in that office. Fewer than a handful of qualified security and safety federal experts are charged with overseeing about 15,000 contractor employees over a 40 square-mile area.

This problem was highlighted by both the Mies and Chiles Commissions. In response, NNSA compounded the problem: rather than beefing up the Los Alamos Site Office, NNSA starved it and turned much of its oversight authority over to the contractor. The proper solution would be to install a robust team of qualified safety and security personnel who are empowered

to oversee and enforce contractual requirements – and who are rewarded for doing so. This means NNSA Headquarters needs to make it a priority to fund these efforts, and to promote federal employees who are thorough in their work.

You also have before you today two men who have collectively issued hundreds, or even thousands, of recommendations for improving security and safety at the labs – DOE Inspector General Greg Friedman and Director of the Department of Health, Safety and Security (HSS) Glenn Podonsky. Yet no one is held responsible at NNSA for implementing their recommendations. Why do we keep asking the Inspector General and HSS to investigate and audit these sites if their recommendations fall on deaf ears? The problems we are discussing today are far from new. In fact, they are infuriatingly familiar.

Inspector General Friedman has offered twelve detailed recommendations for computer-security, as well as a number of recommendations to improve the personnel security clearance process, in the most recent Los Alamos case alone.[3] Officials at NNSA or Los Alamos should be held accountable if these recommendations are not implemented, or at least be forced to present a convincing argument to justify why they have not done so.

In addition to creating an incentive for federal overseers to do their jobs, we also need to make Lab officials feel the consequences when there are failures. The surest way of doing so is to hit the contractor's pocketbook. The problem is that the current fee structure does not reflect the importance of both safety and security. Of the $51 million on the table for FY 07, currently only about $3 million of that amount is tied to security. Fortunately, that small percentage of the fee – 6% – is not set in stone and should certainly be revisited and dramatically increased. The Performance Incentive Fee should be recalculated and equally weighted to reflect the equal importance of accomplishing the mission, ensuring security, and doing so safely. Currently,

---

[3] *Selected Controls Over Classified Information at the Los Alamos National Laboratory*. Special Inquiry Report to the Secretary, Audit Number OAS-SR-07-01. U.S. Department of Energy Office of Inspector General. November, 2006.

completing the program is vastly more valued than having strong safety and security systems – even though failures in safety and security have repeatedly and adversely affected programs. Those incentives should be changed. At the very least, it is clear that DOE should cut the Performance Incentive Fee for the most recent security debacle at Los Alamos.

Another tool that should be utilized is the cost-reimbursement nature of the Los Alamos contract. HSS Director Podonsky currently has a team of investigators at Los Alamos focusing on enforcing the Price-Anderson Act and trying to determine whether or not to assess a penalty for failure to uphold security standards. Historically, such penalties have generally been small in comparison to the fees the contractors receive, and therefore create little incentive for improvement. This is an opportunity to show the Lab how seriously the government takes safety and security: DOE should disallow costs associated with Los Alamos' failure to perform adequately.

POGO also recommends that the "at will" employment provision at Los Alamos be changed. This type of employment creates a clear disincentive for Lab employees who try to raise concerns: if an employee is the bearer of bad news to management, the employee can be fired "at-will." Having seen this scenario play out repeatedly over the last few years, it is no wonder that problems fester until they explode. There is no incentive for the employees to step forward given the tenuous nature of their employment. Furthermore, although this "at will" employment policy is not in effect at Livermore, the employee union is very concerned it might be imposed on them if UC wins the contract competition.

Another recommendation is for Congress to audit the missions currently being conducted at Los Alamos. Few people on Capitol Hill are aware of the various missions being performed there. Is the disparate nature of the Lab's work making it harder to maintain excellence in safety and security? Is the science being conducted reflecting the Congress' sense of the most urgent priorities that could be tackled by these scientists? For decades, Los Alamos has operated as a sacred cow with no serious oversight. I hope this is the beginning of a new era.

In closing, I would like to alert you to the fact that DOE will soon be submitting a request for $150 billion to fund a wildly ambitious project to revamp the nuclear weapons complex, known as Complex 2030, which will include creating the capacity to produce 125 new warheads per year. This Reliable Replacement Warhead (RRW) is envisioned to be a new and "more usable" nuclear warhead. Over the past decade, despite hearing after hearing, report after report, commission after commission, the complex has been unable to fix the egregious security and safety failures that have plagued it. There is no reason to believe that the situation will improve under this new plan. Before any funding for further expansion is approved, the security of the current complex and the safety of its workers must be ensured.

>>To: Derek Dinwiddie <derekd@lanl.gov>, "James L. Tingey"
<jtingey@lanl.gov>,
>> "M. E. Pansoy-Hjelvik" <meph@lanl.gov>,
>> "Keith W. Fife" <kfife@lanl.gov>,
>> "Tammy M. Dominguez" <tammy@lanl.gov>
>>Cc: "Thomas J. Lex" <tlex@lanl.gov>
>>Subject: Suspension of all Classified Computing Activities
>>From: Shean Monahan <spm@lanl.gov>
>>Date: Wed, 10 Jan 2007 13:52:47 -0700
>>X-Mailer: Apple Mail (2.752.2)
>>X-PMX-Version: 4.7.1.128075
>>
>>Derek, Jim, Lisa, and Keith
>>
>>I just got off a conference call with Bob McQuinn concerning the Cyber

>>Security audit that was suspended last night.
>>
>>As a result of the preliminary findings of that audit, LANL has agreed
to
>>suspend all non-essential classified computing activities for at least

>>the next 48 hours by the close of business today. The definition of
>>"non-essential" has been left to the system owners to determine.
However,
>>Bob McQuinn's guidance is simply to suspend all activities, and if you

>>believe certain classified computing activities are essential that you

>>need to make the case to him and get agreement prior to continuing.
>>Classified computing associated with MCA/Safety concerns/Regulatory
>>compliance have a stronger chance of being allowed to continued, as
>>oppose to programmatic needs. Again the status of the AD-NHHO must be
>>determined by COB today.
>>
>>
>>Shean Monahan
>>Nuclear Criticality Safety
>>Phone: 5.7567
>>Pager: 4.1813
>><mailto:spm@lanl.gov>spm@lanl.gov
>>
>
>Tom Lex
>Safety Basis Director
>6-2269
>

JERRY LEWIS, CALIFORNIA, Chairman
C. W. BILL YOUNG, FLORIDA
RALPH REGULA, OHIO
HAROLD ROGERS, KENTUCKY
FRANK R. WOLF, VIRGINIA
TOM DELAY, TEXAS
JIM KOLBE, ARIZONA
JAMES T. WALSH, NEW YORK
CHARLES H. TAYLOR, NORTH CAROLINA
DAVID L. HOBSON, OHIO
SHERWOOD L. BOEHLERT, NEW YORK
HENRY BONILLA, TEXAS
JOE KNOLLENBERG, MICHIGAN
JACK KINGSTON, GEORGIA
RODNEY P. FRELINGHUYSEN, NEW JERSEY
ROGER F. WICKER, MISSISSIPPI
TODD TIAHRT, KANSAS
ZACH WAMP, TENNESSEE
TOM LATHAM, IOWA
ANNE M. NORTHUP, KENTUCKY
ROBERT B. ADERHOLT, ALABAMA
JO ANN EMERSON, MISSOURI
KAY GRANGER, TEXAS
JOHN E. PETERSON, PENNSYLVANIA
VIRGIL H. GOODE, JR., VIRGINIA
JOHN T. DOOLITTLE, CALIFORNIA
RAY LAHOOD, ILLINOIS
JOHN E. SWEENEY, NEW YORK
DON SHERWOOD, PENNSYLVANIA
DAVE WELDON, FLORIDA
MICHAEL K. SIMPSON, IDAHO
JOHN ABNEY CULBERSON, TEXAS
MARK STEVEN KIRK, ILLINOIS
ANDER CRENSHAW, FLORIDA
DENNIS R. REHBERG, MONTANA
JOHN R. CARTER, TEXAS
RODNEY ALEXANDER, LOUISIANA

# Congress of the United States
## House of Representatives
## Committee on Appropriations
## Washington, DC 20515–6015

DAVID R. OBEY, WISCONSIN
JOHN P. MURTHA, PENNSYLVANIA
NORMAN D. DICKS, WASHINGTON
MARTIN OLAV SABO, MINNESOTA
STENY H. HOYER, MARYLAND
ALAN B. MOLLOHAN, WEST VIRGINIA
MARCY KAPTUR, OHIO
PETER J. VISCLOSKY, INDIANA
NITA M. LOWEY, NEW YORK
JOSE E. SERRANO, NEW YORK
ROSA L. DELAURO, CONNECTICUT
JAMES P. MORAN, VIRGINIA
JOHN W. OLVER, MASSACHUSETTS
ED PASTOR, ARIZONA
DAVID E. PRICE, NORTH CAROLINA
CHET EDWARDS, TEXAS
ROBERT E. "BUD" CRAMER, JR., ALABAMA
PATRICK J. KENNEDY, RHODE ISLAND
JAMES E. CLYBURN, SOUTH CAROLINA
MAURICE D. HINCHEY, NEW YORK
LUCILLE ROYBAL-ALLARD, CALIFORNIA
SAM FARR, CALIFORNIA
JESSE L. JACKSON, JR., ILLINOIS
CHAKA FATTAH, PENNSYLVANIA
ALLEN BOYD, FLORIDA
STEVEN R. ROTHMAN, NEW JERSEY
SANFORD D. BISHOP, JR., GEORGIA
MARION BERRY, ARKANSAS

CLERK AND STAFF DIRECTOR
FRANK M. CUSHING

TELEPHONE:
(202) 225-2771

September 21, 2006

The Honorable Samuel W. Bodman
Secretary of Energy
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

Dear Secretary Bodman:

As you know, the Committee included a provision in the Energy and Water Development Appropriations bill for fiscal year 2004, and in subsequent fiscal years, mandating the competition of the management and operating contracts for Ames Laboratory, Argonne National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, and Los Alamos National Laboratory. I am very disappointed with the results of the contract competitions that the Department has conducted to date. The Berkeley and Argonne contracts had no competing bidders. While I hope that the competitive process has yielded some efficiencies and improvements that will benefit the federal taxpayer, those changes will be modest at best. However, I do have some confidence that the Office of Science conducted fair competitions for these laboratory contracts, and will do the same for the upcoming Ames Laboratory competition. With both Berkeley and Ames laboratories being an integral part of university campuses, it is not surprising that other entities are reluctant to bid against the incumbent university contractors.

I am more disturbed by the process that was used to compete the Los Alamos contract. Granted, there were two viable competitors for that contract, and the incumbent University of California was motivated to team with other partners. However, other potential competitors for the Los Alamos contract were discouraged from bidder because of the perception that the Department was determined to award the contract to the incumbent. Potential competitors believed that the Department structured the Request for Proposals for Los Alamos to favor the incumbent contractor and limit the chances of any other competitor winning that contract. That perception proved to be correct.

Unfortunately, that same perception is now prevalent in the contractor community with regards to the pending competition for the Lawrence Livermore National Laboratory. I have had potential competitors inform me that their companies will not invest the time, effort, and expense to prepare a proposal for the Livermore contract because they believe that the Department is determined to award the Livermore contract to the University of California. Unlike the Berkeley and Ames laboratories, Lawrence Livermore is not directly connected to a university campus, and there is no good reason that the Department should not be able to attract multiple qualified bidders on the Livermore contract.

In mandating competition, it was the intent of Congress to attract the widest possible group of interested bidders to bring in fresh ideas and new talent to support the Department's mission. Unfortunately, the Department of Energy's national laboratories are not viewed as a competitive marketplace but as a playground for political patronage. The Department of Energy has resisted moving in the direction of fair and open competitive processes. Unfortunately, the Department has insisted on using the flawed Los Alamos competition as a model for the competition for the Livermore contract, which telegraphed to the contractor community that innovative ideas and concepts would not be favorably received.

The DOE has implemented these historic laboratory competitions in a manner that minimizes the opportunities for real transformation of the DOE laboratory complex. If the Department is unable to develop a Request for Proposal for the Livermore competition that is written to ensuring the most competitive process possible for the procurement, then Congress will have to legislate a delay in the contract competition to give the DOE more time to structure the competition to be completely fair and open, with a priority put on attracting the widest possible group of interested bidders. We need a procurement process that fosters greater competition, not a process that essentially guarantees the status quo.

Sincerely,

David L. Hobson
Chairman, Energy and Water Development
Appropriations Subcommittee

**Statement of Thomas P. D'Agostino**
**Acting Administrator**
**and**
**Deputy Administrator for Defense Programs**
**National Nuclear Security Administration**
**U.S. Department of Energy**
**Before the**
**House Committee on Energy & Commerce**
**Subcommittee on Oversight & Investigations**

**January 30, 2007**

My name is Thomas P. D'Agostino. I am the Acting Administrator of the National Nuclear Security Administration (NNSA), within the U.S. Department of Energy (DOE), a position I have held since January 20, 2007, upon the resignation of Ambassador Linton F. Brooks. I realize that one of the primary reasons I am in this position is because of the Secretary of Energy's dissatisfaction with progress in management and security issues, notably related to Los Alamos National Laboratory (LANL).

Let me be clear, all options for both penalties and motivation are under consideration with LANL. This is not an academic exercise with a nominal fee at stake—the maximum available annual fee for operating LANL, with safety and security as key factors, is over $70 million. The majority of LANS's fee is at risk as is their ability to earn additional award terms. The combination of award fee and award term are powerful incentives on performance and I intend to fully utilize these in managing the contractor. The Department is conducting a review of the incident to determine whether a Notice of Violation will be issued. Finally, the contract has a clause called

"Conditional Payment of Fee, Profit, and Incentives." This clause allows for the complete elimination of fee in the event of a serious safety or security event that results in the loss of life or grave and irrecoverable harm to the security of the United States.

I am serious about my new responsibility for security across the nuclear weapons complex. In fact, my first two days on the job as Acting Administrator were spent in New Mexico at LANL and the Los Alamos Site Office (LASO) to get a first hand, upfront and personal appreciation of the issues and to talk with the people responsible for implementing improvements. I was at the Site Office to see the staff and personally explain my recent decision to reassign the Site Office Manager, Ed Wilmot. In Mr. Wilmot's place, I have directed one of the Department's most experienced Site Office Managers, Mr. Dan Glenn from the Pantex Site Office in Amarillo, Texas, to serve as the Acting LASO Manager until a permanent replacement is found. Mr. Glenn has extensive safety and security experience at one of our most sensitive facilities; in fact, Pantex is the only NNSA facility where we have complete nuclear weapons on-site. LANL is also a unique place with some of the world's best science and most sensitive information, and I will support LASO with the best team to continue to drive improvements and make sure we are getting the job done.

On January 3, 2007, I notified the LANS Board of Governors Executive Committee that I was calling the Executive Committee to Washington, D.C. that following week. On January 10, I met with the Executive Committee and told them of my concern in how they have handled the current security incident at LANL. The

Secretary, Deputy Secretary, NNSA Administrator, and LASO Manager joined me to emphasize the seriousness of the situation. In the coming months I will be routinely meeting with members of the Executive Committee to hear how they will to improve the security culture at LANL. Additionally, I have asked the Chairman of the Board of Governors, Mr. Gerald L. Parsky, to call the Secretary on a regular basis to update him personally on actions that the Board was taking to reach back to the corporate parents to support improvements at the laboratory.

Make no doubt about this—if the current laboratory management is unable or unwilling to change the security culture at LANL, I will use every management tool available to me, consistent with the terms of the LANL contract, including recompeting the contract if necessary.

All NNSA security functions, with the exception of cyber security, are consolidated under the NNSA Associate Administrator for Defense Nuclear Security. All NNSA cyber security issues are consolidated under the NNSA Chief Information Officer, who reports to the NNSA Associate Administrator for Management and Administration.

With respect to the current issue of security at Los Alamos, let me assure you that NNSA is committed to the security of our nuclear weapons, nuclear material, and classified matter and it has taken significant steps to improve security since its inception. Neither NNSA nor I take any breach of security lightly.

The nature of our classified operations is complex, but the elements of good security are not. Good information security entails clear rules, strong controls, testing and validating, which provides for a credible deterrence. Personnel security clearances determine who gets access to classified information. Building and security area access controls provide high confidence that people going in and out of classified work areas are authorized to be there. Information security controls work to ensure only people with a need to know have access to the information.

While these controls help set the foundation for a good security program, the system must also provide deterrence against violation of the rules and controls; a high probability for the discovery of security violations; and strong sanctions for willful or negligent violations. While we expect that security-cleared employees will abide by security rules because they understand and value good security, the system must also provide credible deterrence against intentional or inadvertent violations of the system of rules and controls. Searches and work area spot checks help ensure the system is operating as designed across all levels of the operation. We must continue to strengthen these activities. Specifically, LANL has strengthened its security escort requirements and more clearly specified the expectations and requirements for their escort program. LANL has also increased the number of inspections of personnel entering, working in, and exiting security areas and have conducted nearly 5,000 additional inspections since this incident came to light.

While the Secretary has commissioned a special task force to review the Department's personnel security program, NNSA has been taking action over the past year and a half to improve our personnel security processes. Specifically, we re-engineered work practices to reduce clearance processing time, implemented the electronic questionnaire for investigations processing (e-QIP), strengthened our quality assurance mechanisms, and instituted metrics to monitor and report on the performance of our personnel security functions. Additionally, we have coordinated with the Defense Security Service to provide comprehensive clearance adjudication training to our nearly 100 contractors and Federal personnel security professionals at the NNSA Service Center.

During the past two years, NNSA has made changes to strengthen the cyber security posture across the national complex and more recently addressed issues identified by the LANL incident. During 2005, the Department developed the strategic plan and a deployment schedule for Diskless Workstation implementation. In 2006, the Agency appointed Designated Approving Authorities (DAAs) for each NNSA site and are dedicated solely to cyber security, policy oversight and inspection.

NNSA has also assembled its Federal cyber security experts from across the Complex to inspect all Vault Type Rooms at LANL to determine their compliance with the Department's directive to close vulnerable system data ports. We have also set in place a schedule for this team to inspect the cyber security implementation at all other NNSA sites. Based on these inspections I plan to take aggressive actions to strength our

cyber security and I pledge to you that I will deal as swiftly and directly with any incidents or actions needed to improve the cyber security posture of the NNSA.

I would like to highlight some of the actions NNSA has taken to improve security, most notably those taken since the last significant security incident at Los Alamos in 2004, involving Classified Removable Electronic Media (CREM).

NNSA completed two major studies of NNSA security, one led by Admiral (Retired) Hank Chiles and one led by Admiral (Retired) Rich Mies. Admiral Chiles' report in March 2004, "Strengthening NNSA Security Expertise: An Independent Analysis," provided recommendations to make our Federal security workforce more effective. Admiral Mies' study in April 2005, "NNSA Security: An Independent Review," provided more than 100 recommendations in thirteen programmatic areas, including physical security, cyber security, intelligence and counterintelligence and making recommendations ranging from program management to budgeting to oversight.

In response to the Chiles report:

- Our Federal Site Offices have implemented formal security training programs leveraging the Departments Technical Qualification Program and the DOE National Training Center's Professional Enhancement program.
- We established a security intern program and have successfully integrated it into the Department's Future leaders Program.

Likewise, we took effective action to implement the recommendations of Admiral Mies:

- Partnered with DOE's Office of Health, Safety, and Security to review our security policies with the goal to make our policies consistent with national standards, clearly understandable, and effective when implemented;
- Re-aligned Defense Nuclear Security staff roles and responsibilities to improve security program planning, programming, and evaluation;
- Issued a Performance Assurance Program, which provides a multi-tiered system of self-assessments and other reviews of security performance aimed at assuring comprehensive assessments of security programs;
- Established the Defense Nuclear Security Leadership Council, which comprises all site office security directors and meets regularly to address overarching security implementation challenges; and
- We actively disseminate lessons learned from incidents and inquiries and the Associate Administrator for Defense Nuclear Security has directed the establishment of a Security Lessons Learned Center which will enhance our information sharing.
- Replaced several Federal security directors for sub-standard performance.

We have received a number of reports from the Government Accountability Office, the DOE Inspector General, and the DOE Office of Independent Oversight. Like the Chiles and Mies studies, we have addressed the recommendations in these reports and have made major improvements.

However, we do not rely on others to identify ways to improve security. You will recall that in 2005, the Administrator announced his intention to stand up an NNSA Headquarters Security Oversight Office. Over the course of 2005 and 2006, that office has been staffed and has begun conducting regular and special reviews to ensure the effectiveness of our security programs and security line management. This office is also implementing our new risk management model and the oversight of security planning and vulnerability analysis. It has improved our responsiveness to outside recommendations, reduced the number of open findings, and reduced the number of security incidents across the complex through more effective sharing of best practices and lessons learned. This year we will begin our first review of Site Office oversight processes as part of an initiative to improve our local Federal security oversight even more.

Again, I take these most recent events at LANL very seriously. I welcome suggestions on how to best proceed at LANL and want to have a national laboratory that is known best for its outstanding contributions to national security and the advancement of science.

## Summary of Statement by Gregory H. Friedman, Inspector General

Secretary Bodman requested that the Office of Inspector General begin a review of the possible compromise of classified information at the Los Alamos National Laboratory.

Our special inquiry disclosed that computer ports, which could have been used to inappropriately migrate information from classified systems to unclassified devices and computers, had not been disabled; classified computer racks were not locked; individuals were inappropriately granted access to classified computers and equipment; computers and peripherals that could have been used to compromise network security were introduced into a classified computing environment without approval; and, critical security functions had not been adequately segregated.

In many instances, Laboratory management and staff had not developed policies necessary to protect classified information. Further, Laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and inspections. Our findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

We provided the Department with a number of specific recommendations designed to assist it in its efforts to correct identified deficiencies. In addition, at the request of the Subcommittee, we identified several broader actions that could improve the overall security climate at Los Alamos.

Friedman

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on the Office of Inspector General's review of the recent compromise of classified data at the Department of Energy's Los Alamos National Laboratory.

## BACKGROUND

The Los Alamos National Laboratory, now operated by Los Alamos National Security, LLC, for the Department's National Nuclear Security Administration (NNSA), has been at the forefront of our country's national security-related research and development enterprise for over 60 years. The physical and intellectual data that resides at the Laboratory reflects its critically important missions, which range from ensuring the safety and reliability of our nuclear stockpile and preventing the proliferation of weapons of mass destruction to protecting the Nation from terrorist attacks. To support these missions, the Laboratory manages highly sensitive classified materials and information. Safeguarding such classified information – housed at over 2,700 separate classified computing operations, including 139 vault-type rooms – requires that the Laboratory establish and maintain strong security controls.

Over the years, there have been a number of highly-publicized security incidents that have cast doubt on the Los Alamos National Laboratory's ability to protect classified national security assets. In 1999, a Los Alamos scientist was accused of and subsequently pled guilty to mishandling classified information by downloading nuclear secrets and removing them from the Laboratory. In the following year, largely in response to security concerns at Los Alamos, the NNSA was established as a semi-autonomous agency. In 2002, two computer

hard drives containing classified data were thought to be missing from a secure area within the Laboratory, but were later found. In 2004, after an inventory indicated that two computer disks containing classified information were missing, the Director of the Laboratory ordered a lengthy stand-down to address and resolve security concerns. That stand-down, according to the U.S. Government Accountability Office, delayed important national security work at a substantial cost to the taxpayer.

Because of the need to ensure that the Nation's vital nuclear material and information are adequately protected, the Office of Inspector General has performed numerous audits, inspections, and investigations of physical and cyber security-related issues at the Laboratory. Our reviews have covered diverse areas such as the implementation of the design basis threat, safeguards over classified material and property, and the security of information systems. I have been asked to testify before this Subcommittee and other Congressional panels on several occasions regarding a series of management and security issues at Los Alamos.

As has been well-publicized, on October 17, 2006, the Los Alamos County Police Department responded to a call at the home of a former employee of a Laboratory subcontractor. During a subsequent search of the residence, police seized a computer flash drive that contained electronic images of Los Alamos classified documents. In addition, hard copies of over 200 classified documents belonging to the Laboratory were also found in the residence. Laboratory officials determined that the seized classified information was derived from an ongoing scanning and archiving project. This scanning project was being performed by a subcontractor to the Laboratory. A criminal investigation regarding the seized material was

initiated by the Federal Bureau of Investigation. Shortly after the investigation began, the Secretary of Energy requested that the Office of Inspector General perform a separate review of the possible compromise of classified information at the Los Alamos National Laboratory. The Secretary also asked that we evaluate certain aspects of the Department's security clearance process.

## OFFICE OF INSPECTOR GENERAL REVIEW

The Office of Inspector General promptly began a special inquiry that focused on what the Department and its contractors did or did not do to protect classified information and the steps that were taken to ensure that only properly qualified individuals had access to such information. As part of that effort, we interviewed over 80 Departmental, Laboratory, and subcontractor personnel; reviewed relevant security guidance and procedures; and, examined numerous other relevant documents. Our findings related to the security clearance process should be discussed in closed session.

Our special inquiry revealed that despite the expenditure of millions of dollars by the NNSA to upgrade various components of the Laboratory's security apparatus, the security environment at the Laboratory was inadequate.

In particular we found that:

- Certain computer ports, which could have been used to inappropriately migrate information from classified systems to unclassified devices and computers, had not been disabled;
- Classified computer racks were not locked;
- Certain individuals were inappropriately granted access to classified computers and equipment to which they were not entitled;

  Computers and peripherals (scanners and a printer) that could have been used to compromise network security were introduced into a classified computing environment without approval; and,

  Critical security functions had not been adequately separated, essentially permitting system administrators to supervise themselves and override controls.

In many cases, Laboratory management and staff had not developed policies necessary to protect classified information, had not enforced existing safeguards, or provided the attention or emphasis necessary to ensure protective measures were adequate. Some of the security policies were conflicting or applied inconsistently. We also found that Laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and physical inspections. In short, our findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

Any diversion of classified material creates a potentially serious national security situation. For this event in particular, the full extent of damage or dispersion of the classified material

may never be fully known. The criminal investigation into this matter is ongoing and may yet reveal additional security problems. Our findings, however, which are discussed in more detail in the following paragraphs, underscore continuing problems with the Laboratory's overall management and security posture.

### Open Computer Ports

Following the security incident in 1999, the then Secretary of Energy ordered the Los Alamos National Laboratory and other similarly situated facilities to implement controls and protections to make it physically impossible to migrate classified information to unclassified systems or devices. Although Los Alamos had taken action to disable some devices, our review found that, in a significant number of instances, the Laboratory failed to deactivate unneeded open computer ports such as USB and "firewire" ports that could have been used to circumvent security controls.

This weakness could have permitted the transfer of classified information to unclassified systems or easily concealable devices such as flash drives and portable hard drives. Open and unsecured ports also could have ultimately been used to transfer classified information to the Laboratory's unclassified network and the Internet. As evidenced by a series of e-mail exchanges in the March/April 2006 timeframe, officials in the Laboratory's Chief Information Officer's organization recognized that it would be a simple matter to exploit this weakness by plugging a USB or firewire recording device into an open port and copying information to it. However, despite this recognition, a Laboratory-wide solution was never developed or deployed.

### Unlocked Computer Racks

We also noted that Laboratory system administrators failed to take advantage of readily available security measures that, in this case, could have helped prevent the unauthorized removal of the electronic classified material found on the seized flash drive. As part of an initiative to secure classified removable electronic media (CREM) following the 2002 security event, Los Alamos acquired locking mechanisms that were to be used to secure and prevent access to most rack-mounted classified computer systems. Following the installation of the locks, Laboratory management determined that if a computer system did not contain CREM and it was located in a vault-type room, there was no need to lock the racks. As a consequence, racks housing classified computers in the vault we reviewed were never secured. Based on our inquiries, a Laboratory management official conceded that using the available locks would have denied access to the enabled USB ports and could have prevented the download of the diverted classified information.

### Inappropriate Access Granted

In addition, despite existing control measures and specific guidance by the NNSA to the contrary, system administrators at the Laboratory inappropriately granted certain individuals access to classified computer equipment to which they were not entitled. Specifically, individuals were given authority to physically access rack-mounted classified computer systems – access that could have permitted them to exploit open USB and firewire ports. Laboratory officials also allowed a person that had no need to print documents to use a high-speed classified network printer capable of producing double-sided documents identical to the

format of the hard copy classified documents that had been seized by law enforcement officials. A senior Laboratory security official confirmed that granting unneeded access to users was contrary to policy and that such action endangered security.

### Introduction of Unapproved Devices

To ensure that classified systems are secure to operate, computers and peripheral devices should be evaluated for risk and included in an approved systems security plan prior to being introduced into a classified computing environment. However, program, security, and system administration officials responsible for the vault we reviewed routinely ignored these controls. Our review disclosed that officials permitted the introduction of several computers and peripheral devices (scanners and a printer) into a classified computing location even though these devices were not included in the accredited security plan. Thus, Laboratory and Federal officials were not able to evaluate the security implications of their inclusion in the vault in question. Potentially, the introduction of these devices could have compromised security.

### Incompatible Security Functions

Additionally, Los Alamos did not adequately separate critical security duties. According to NNSA policy, "*measures must be implemented to ensure the management, control, and separation of security critical functions.*" However, Laboratory officials frequently did not provide for such separation, and a single individual was tasked with both system administration and security officer duties – essentially supervising and approving his or her own actions. As a result, the system administrator was able to provide access to classified computers and peripherals to unauthorized individuals, thereby overriding classified

protection safeguards. Los Alamos officials noted that the same issue existed in classified computing venues across the Laboratory.

## ADDITIONAL FACTORS CONTRIBUTING TO DIVERSION

The security weaknesses we discovered resulted from control and management breakdowns at both the contractor and Federal level. While the Department, the NNSA, and Los Alamos had deployed some security controls to protect classified information, we observed problems with policy development and implementation. Had the Department and the NNSA been more aggressive in its contract administration and review activities, it may have been able to prevent, detect, or correct in a timely manner the problems or factors that contributed to the diversion of classified material.

### Weaknesses in Security Policies

Our review, for example, disclosed a particularly significant instance where classified computer policies had not been developed or properly formalized. In 1999, the then Secretary of Energy directed that safeguards be developed and implemented to prevent the migration of classified data to unclassified systems to protect against insider threats. That direction specifically required that organizations "*establish requirements that place stringent controls on computers and work stations, including controls on...ports that could be used to download files*." The requirement was never included in the Department's cyber security policy nor was it completely implemented by the Laboratory.

Furthermore, our inquiry revealed that conflicting direction and a lack of understanding regarding the introduction of equipment into classified computing environments contributed to the weaknesses we found. For example, Laboratory guidance required that security plans be updated and systems reaccredited when security configurations changed. Certain officials, however, incorrectly instructed security officers that there was no need to comply with that direction for selected devices. In other instances, officials inappropriately believed that the need to update security plans and obtain reaccreditation of classified systems was a matter solely within their discretion. They held this mistaken belief even though the Laboratory had published specific guidance regarding events that triggered update requirements. During our review, we identified a number of changes in security configurations for the vault we evaluated that should have triggered the requirement to update the system security plan. Yet, such action had not been taken.

Policy regarding the acquisition of computer support services for classified computing environments at the Laboratory was also inconsistent. In particular, as it applies to the matter under review, procurement policy permitted subcontractors to furnish unaccredited items such as scanners and software for archiving projects. Such practices, however, were contrary to the system's security plan and to cyber security guidance issued by the NNSA. The NNSA guidance specifically prohibited the connection of non-government owned equipment to classified networks.

**Insufficient Management Review and Overdue Inspection Activities**

The failure of Laboratory managers and Federal security officials to perform verification activities may also have adversely affected the classified security climate at the Laboratory and contributed to the recent removal of classified material. Laboratory security officials indicated that they did not visit vaults or computing facilities to determine whether controls described in security plans were actually in place. Federal officials at the Los Alamos Site Office also told us that they did not conduct physical inspections of the Laboratory's classified information systems. Accrediting officials at the Site Office explained that they placed a great deal of emphasis on reviewing security plans and accrediting systems, but that they had only 1.5 staff years to dedicate to classified security. They asserted that as a consequence they were unable to perform physical inspection of systems to validate that the Laboratory's plans were accurate and were being enforced.

Delays in completing classified information system inspections may also have impacted the detection of the security weaknesses we identified. NNSA officials informed us that they relied almost exclusively on the Office of Independent Oversight, Office of Health, Safety and Security to conduct detailed inspections of Los Alamos' classified information systems. These inspections are normally completed once every two years. However, the inspection at Los Alamos had not been performed for about four years for a variety of reasons including the 2004 security stand-down at the Laboratory. The Office of Independent Oversight had begun a previously scheduled review of Los Alamos' classified information systems at about the same time the diversion of classified information was discovered.

**NEEDED ACTIONS**

After this incident was discovered, management officials at various levels of the Department and at the Laboratory launched several efforts to identify and correct control deficiencies that caused or contributed to the unauthorized removal of classified information. In particular, the Secretary established two task forces to address our findings and the Deputy Secretary directed an immediate review of policies and practices related to computer ports at each of the Department's facilities.

As a result of our review, we provided the Department a number of recommendations designed to assist it in its efforts to correct identified deficiencies. For example, we recommended that the Department take immediate action to disable unneeded computer ports, secure classified computer racks, segregate critical security functions, and limit classified computer access and privileges to those who specifically require it.

In its letter of invitation, the Subcommittee requested that the Office of Inspector General identify broader actions that could improve the overall security climate at the Los Alamos National Laboratory and the Department at large. Based on the results of this special inquiry and other recent IG reviews and investigations, we concluded that the Department and the NNSA should:

1. Establish an up-to-date, unified, risk-based security policy that flows throughout all elements of the Department. It is essential that this policy be applied consistently and

that all aspects of security -- physical, cyber, and personnel -- be integrated to ensure a seamless system.

2. Aggressively hold individuals and institutions -- at the Federal and contractor levels -- accountable for failure to follow established security policies. Penalties should include meaningful reductions in contractor fees; personnel reassignments and terminations; civil penalties; program redirection; and, ultimately, should need be, contract termination.

One final note, one of the most disturbing aspects of this event is the fact that it was not discovered by the Laboratory but by local police during an off-site investigation unrelated to Laboratory activities. Without this inadvertent discovery, the diversion of classified material may never have been disclosed. In that light, Los Alamos and the Department need to strengthen efforts to proactively detect and prevent security breakdowns. This might include, for instance, improving the level of monitoring of classified computer/information activity by the use of specialized software, activity logging, and by initiating a program of unannounced security checks beyond routine inspections. Admittedly, there is a cost involved with such undertakings, but it is a cost that may be necessary given the pattern of security issues at the Laboratory.

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

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

January 30, 2007

Mr. Chairman and members of the subcommittee, thank you for inviting me to testify today as you probe into the security violation involving the improper removal of classified information from the Los Alamos National Laboratory. To perform its national security mission, the Department of Energy produces, processes, and stores significant quantities of classified material on a continuous basis. Because of the nature of this information and its potential impact on the national security of the country, we need to ensure that our policies and practices minimize the risk of potential security failures.

In light of the progress made in the last few years throughout the Department to correct past performance deficiencies in the control of classified information, this most recent unauthorized removal of classified information by a cleared employee at Los Alamos is a significant disappointment to the Secretary and the Department. We fully understand that incidents such as the one currently under examination by the Committee not only expose our sensitive national security information to potential compromise, but erode public confidence. As an organization with a mandate for an independent review responsibility, our organization is responsible for assessing performance based on the facts.

Los Alamos has made some progress in the past five years, but we must balance this against what should be the expectation of performance for an organization with such a critical scientific, defense and national security mission. In this respect, Los Alamos has been slow to address the root causes of its failures and to transform the entrenched operational culture that perpetuates them. Los Alamos now has new contractor management and an opportunity to move in a more positive direction.

At the time this specific incident was discovered, the Office of Independent Oversight was conducting a scheduled comprehensive inspection of the Laboratory's safeguards and security, cyber security, and emergency management programs, including those responsible for protecting classified information. Consequently, the Office of Independent Oversight was not assigned responsibility for conducting the inquiry into the circumstances surrounding the incident. This responsibility was assigned to the Inspector General. I will therefore focus my remarks on the overall performance of the programs we observed during the Independent Oversight inspection of Los Alamos National Laboratory.

Prior to our recent inspection activity, we conducted inspections of safeguards and security, cyber security, and emergency management programs at Los Alamos in 2002. The 2002 safeguards and security inspection determined that the Laboratory's Material Control and Accountability program was performing at less that an effective level of performance. During the concurrent cyber security inspection, the classified cyber security program was determined to be performing effectively, consistent with DOE requirements; however, the unclassified cyber security program exhibited significant weaknesses.

Independent Oversight's 2006 comprehensive inspection of Los Alamos also covered the areas of safeguards and security, cyber security, and emergency management in compliance with current Independent Oversight protocols. On-site activities for the 2006 inspection concluded last month. The final inspection report is currently under review and has not yet been published. Although the final report has not been issued, we can provide a brief general summary of the major inspection results in terms that are appropriate for this unclassified hearing.

Safeguards and Security Programs

During this inspection, the Laboratory's safeguards and security programs exhibited both strengths and weaknesses. While we are encouraged by limited improvements in some areas, we believe that considerable work remains to be done to ensure that safeguards and security programs at Los Alamos fully meet Department expectations.

Protection of Special Nuclear Material

Our inspection concluded that Los Alamos is adequately protecting the Category I quantities of special nuclear materials. This is based on our observations of effective performance in several critical areas, including improved performance in some functions that had previously exhibited weakness in 2002. The most significant improvement in the protection of special nuclear materials can be attributed to the collective actions of the Department, NNSA and Los Alamos to remove weapons grade quantities of this sensitive material from Technical Area 18, which had been the target of much public criticism for several years regarding its questionable security posture. The transfer of a significant quantity of material to the Nevada Test Site's Device

Assembly Facility, a substantially more secure facility, has facilitated on-site consolidation of weapons grade materials into a single security area at Los Alamos that affords a more effective protection posture.

Physical security systems installed to protect special nuclear materials at Los Alamos were subjected to rigorous performance testing and evaluation. Though aging, the current Perimeter Intrusion Detection and Assessment System around the facilities processing weapons grade special nuclear material performs effectively, and is adequately maintained.

Our evaluation of the Laboratory's protective force identified improvements since the 2002 inspection. Many of these are attributed to the aggressive steps taken to meet Departmental security goals by the end of FY2006. For example, Los Alamos increased protective force mobility, survivability, and lethality (e.g., procurement and deployment of enhanced weapons systems and armored vehicles). Protective force members performed effectively in both Limited Scope and full scale Force-on-Force performance tests. While overall protective force performance was determined to be effective, additional attention is required to improve certain tactical capabilities and communications.

While the Material Control and Accountability Program showed the greatest level of improvement since the 2002 inspection and was deemed to be performing effectively, some program areas require further attention, including the vulnerability assessment process which identifies risks associated with small quantities of nuclear materials maintained outside of the Protected Area. In addition, processes to accurately measure certain nuclear materials that

present unique measurement uncertainties require further work. Continued programmatic support is needed in order to sustain program improvements.

While not currently placing nuclear materials at risk, a few elements of the protection program for special nuclear materials require increased management attention. For example, several aspects of the Human Reliability Program require strengthening. This assurance program monitors the trustworthiness and reliability of employees who perform sensitive duties and require physical access to weapons-usable special nuclear material. Similarly, various aspects of the issuance and retrieval of security badges and the out-processing of employees need to be improved. These elements require increased attention and follow-up by line managers.

Protection of Classified Matter

In the area of classified matter protection it was evident that the site has made significant improvements in its efforts to track and account for Classified Removable Electronic Media and printed documents, is implementing a new electronic lock and key system that will reduce the number of keys and will record key usage, and has implemented a security inquiries program that provides stable leadership, is thorough in its process, and uses results in the form of lessons-learned to avoid recurrence where possible. While certain elements in place to protect classified documents and materials were found to be functioning effectively, we identified a number of significant problems within this program.

It was evident that the site is overly dependent on the use of non-standard storage configurations for the protection of many of its classified weapons parts. Storage of classified weapons parts at Los Alamos does not meet normal protection requirements and therefore required alternative protection measures to adequately compensate for storage configuration shortcomings. Compensatory measures that were specifically established to support approval of these non-compliant storage configurations were found to be inconsistently executed and were therefore not providing adequate protection. Furthermore, the need for additional protection measures was also identified in order to ensure that some classified components were protected from unauthorized visual or physical access. A review of the Technical Surveillance Countermeasures Program, intended to protect against electronic eavesdropping, revealed that the program lacked the resources necessary to provide the levels of support required by the Laboratory and its missions. The overall impact of these and other deficiencies in the protection of classified matter at Los Alamos is considered to be substantial.

Management Feedback and Improvement Mechanisms

With regard to management processes, implementation of important management feedback and improvement mechanisms was seriously flawed at both the Laboratory and the NNSA site office. While the Laboratory has new plans for conducting self-assessments and implementing a contractor Performance Assurance Program as part of the contract transition, the plan has yet to be fully implemented. Neither has the Laboratory implemented an effective process for developing, implementing, tracking, closing, and validating corrective actions for identified deficiencies. Similarly, the NNSA site office's Security Survey Program -- a primary tool for

line management oversight of contractor security performance – also suffers from insufficient resources and inadequate implementation. In a few cases, the Laboratory has decided not to comply with DOE requirements and the Laboratory and NNSA did not utilize the Department's mandated deviation processes to fully assess and accept the risks associated with these decisions. Additional effort is needed to improve performance of management systems, since these areas are essential to attaining and sustaining effective protection programs, not only in the safeguards and security arena but also in cyber security and emergency management programs.

Cyber Security Programs

Independent Oversight also inspected classified and unclassified cyber security programs at the Laboratory. We conducted penetration tests of unclassified systems during the 2002 inspection. However, this most recent inspection was the first time that classified computer systems at Los Alamos were tested in such a rigorous manner. (Independent Oversight was granted specific authority to conduct penetration testing of classified systems by the Deputy Secretary of Energy in 2004).

Some progress in improving Los Alamos cyber security was identified by our inspection team, the most significant of which include the segmentation of computer networks to establish need-to-know protection controls, implementation of measures to mitigate risks posed by wireless technology (on the unclassified network), and the centralization of management responsibility for most information systems. In addition, the unclassified computer network was identified as

deploying a well-configured perimeter defense that successfully mitigates many of the sophisticated threats originating from the Internet.

While progress was evident in certain areas, much improvement is still required to safeguard classified information. Los Alamos' cyber security policies and procedures are not comprehensive and are not up to date with DOE/NNSA requirements or other guidelines, nor do they sufficiently address threats posed by emerging technologies. Additionally, risk management processes are insufficient, resulting in risk acceptance decisions at inappropriate levels of management.

The protection of classified computer systems is overly dependent upon administrative controls rather than on more robust engineered controls and barriers. The existence of such measures would have mitigated the ability of the employee involved in the security incident to perform the actions necessary to remove the data from the classified computer system without authorization. Because the Laboratory has not implemented these measures, Los Alamos national security systems continue to operate at an increased risk from insider threats. My Office has been working with the Chief Information Officer in revising the Department's classified cyber security policy to address emerging technologies and new threats. The Chief Information Officer has made this effort one of his highest priorities.

Another problem area identified at Los Alamos involves the certification and accreditation of both classified and unclassified information systems. Los Alamos certification and accreditation processes have not kept up with current methodologies, and existing processes do not ensure a

consistent approach for applying and testing necessary security controls. There are 25,000 unclassified workstations and servers at Los Alamos not certified and accredited.

Moreover, self-assessment processes are weak, with very few systems actually being tested as part of these assessments. Deficiencies identified during self-assessments are not reported to the Los Alamos Site Office or NNSA, and development of corrective action plans to address them is optional. As a result, there is little in-depth understanding of program weaknesses. It is also of concern that the Los Alamos Site Office and NNSA have not provided sufficient leadership to ensure that all current cyber security requirements are appropriately implemented and that performance is monitored to ensure effectiveness.

While progress has been made to date, the cyber security issues that remain at Los Alamos make it clear that a significant amount of additional work is needed in this area.

Emergency Management Programs

Independent Oversight also conducted an inspection of Los Alamos' emergency management programs. Of the seven focus areas inspected, all were found to exhibit serious weaknesses requiring increased management attention. Inspection results reflected a lack of progress in implementing program improvements for previously identified deficiencies. More disconcerting is the fact that four previous findings, although closed by NNSA, had not been effectively corrected.

Other Related Independent Oversight Activities

Secretary Bodman has requested my office to organize and lead a joint task force to review the Department's overall Personnel Security Program and Policies. As we noted earlier, the recent Los Alamos incident raised DOE management concerns about certain determinations used in granting clearances several years ago. In addition to questioning processes used to adjudicate derogatory information, these concerns also involve the adequacy of follow-up procedures for monitoring and reinvestigation when warranted. This task force will review DOE's personnel security policies and standards and will provide specific findings and recommendations for resolving identified deficiencies. Task force activities are scheduled to be completed by February 28 of this year. In addition to performing these activities in the personnel security arena, my office will also support the Chief Information Officer, who has been assigned by the Secretary to conduct a similar review of the Department's Cyber Security Program. I will defer to my colleague, Mr. Pyke, to elaborate on his plans for the conduct of this cyber security review.

Concluding Remarks

Mr. Chairman and Members of the subcommittee, our recent Independent Oversight inspection resulted in the worst set of performance ratings for safeguards and security, cyber security, and emergency management collectively that we have seen at the Los Alamos National Laboratory in many years. That combined with the history of security problems at Los Alamos is of great concern to everyone. However, it would be an oversimplification to say that everything is wrong at the Laboratory and that they are incapable of protecting national security assets. The recent

inspection indicated that, on balance, special nuclear material and classified removable electronic media, two areas with historical weaknesses, have improved and were adequately protected. Improvements in these and other areas should be considered along with the remaining significant deficiencies identified during the recent Independent Oversight inspection.

Since the time when responsibility for managing site operations was transferred to the new integrating contractor, there is evidence to indicate that the new contractual relationship provides a better foundation for security emphasis. In comparison to past contract management processes, the new contractual arrangements and performance-based award fee structure provide increased incentives for the Laboratory contractor to implement an improved, compliant, and effective security program in the future. However, the overall security picture is still below departmental standards—an obvious conclusion from not only site events but also from the results of our most recent inspection activity. As our organization moves ahead in the continued evaluation of the Laboratory's performance, we are mindful of the issues at Los Alamos and their causes. We are cognizant that productive changes require our continued commitment to identifying the origins of breakdowns in the areas of security, as well as health and safety. We look forward to participating in the continued identification and resolution of Departmental problems, and seek to assist Line Management in pursuing clear paths for successfully implementing corrective actions. We hope to do this through our independent oversight activities.

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

JANUARY 30, 2007

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. I came to the Department in November 2005, and have given a high priority to revitalizing the management of cyber security within DOE.

Over the last year, the Department has undertaken a major effort to improve our cyber security. We developed a plan to update Departmental cyber security directives and to issue guidance in specific areas of cyber security. In December 2006, the Deputy Secretary signed a new DOE cyber security Departmental Order which established a new governance structure for cyber security program management. This Order directs the use of a risk-based management approach and makes clear assignment of responsibility to Under Secretaries and other senior officials to oversee cyber security management within their organizations, including the field organizations under their jurisdiction. The Under Secretaries have accepted this enhanced role, and are working hard to strengthen the management of cyber security.

The new Order provides for timely issuance of urgently needed new cyber security guidance. To date I have issued 15 cyber security guidance documents, and the Office of the Chief Information Officer continues to develop guidance in accordance with the plan developed last year. I have already issued guidance on certification and accreditation of systems and on system configuration management, both directly relevant

to the recent Los Alamos incident. The new Order gives the Department flexibility to respond in a timely way to the changing threat environment and other time-sensitive concerns. For example, we have already issued special guidance on protection of personally identifiable information and on disposal of disk drives.

In direct response to the recent security incident at Los Alamos, the Deputy Secretary signed a memorandum in early November directing that actions be taken quickly to provide more protection of classified systems and the classified information on them. This memorandum included guidance prepared by the Office of the Chief Information Officer on blocking physical ports on classified computers. Our office has also conducted a study that has identified hardware and software means that can be used to block physical ports, or connection points, on computers. In addition, the Secretary has asked me to lead a review of the Inspector General's cyber security recommendations in his report on the recent Los Alamos incident. We expect to complete the report of this review by late February.

Finally, directly to the concerns being addressed in this hearing, we have recently completed a planned DOE National Security Systems Controls Manual, now in formal, final review within the Department. This Manual, which updates the Department's formal directive for protecting classified systems, was already being prepared when the Los Alamos incident became known. We have been able to incorporate actions in the Manual based on a number of the lessons learned from this incident.

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

Statement of Clay Sell
Deputy Secretary
U.S. Department of Energy
Before the House Energy and Commerce Committee
Subcommittee for Oversight and Investigation
January 30, 2007

Chairman Stupak, Congressman Whitfield, and Members of the Subcommittee, I welcome the opportunity to appear before you today to discuss security within the Department of Energy and the recent security incident at Los Alamos National Laboratory (LANL).

The national security responsibilities entrusted to LANL are among our Nation's most important. The successes that have sprung forth from this great lab in years past, and today, are properly a source of great pride and power in our country. The capabilities of the men and women of LANL continue to make this lab still the only place to go for many national security requirements. And, of course, the secrets entrusted to the lab are among our Nation's most sensitive. These are among the reasons that the facts of the most recent security incident at LANL are so troubling and a source of such tremendous frustration and concern to the Secretary, me, and many others throughout the DOE enterprise.

And now, despite years of focused attention and the expenditure of millions of dollars, we are confronted again with a security failure, the facts of which suggest we still have a much larger and deeper problem. Many well-intentioned leaders have worked to improve security at LANL over the last few years. And in many key areas, the Department and the Laboratory have made substantial progress. But Secretary Bodman and I are less interested in effort, process, and good intentions and more interested in results; and the results on matters of security at Los Alamos National Laboratory remain unacceptable.

You have already heard from earlier witnesses about what they think may have led to the problems, and what happened in the recent matter. Later today, you will hear from the Acting Administrator of the NNSA, the Department's Chief Information Officer, and the Director of LANL in more detail. Therefore, I intend to focus the balance of my remarks on what the Secretary and I are doing to fix problems and move forward.

1. In the immediate aftermath of learning about the security breach at LANL, we acted immediately to assess the situation and understand the facts. The NNSA Administrator dispatched the Chief of Defense Nuclear Security and a cyber security team to the site to begin immediate review of the incident. On October 26th, the Secretary ordered the Inspector General (IG) to investigate. And on October 30th, I personally traveled to the Lab to meet directly with those on the ground and to gain

first-hand knowledge of the incident to begin remedial actions to address the problems.

2. We took quick action to address realized vulnerabilities. On November 8th, I issued a memorandum to improve cyber security protection for classified computer systems throughout the DOE complex. That memo included immediate direction to every lab and DOE facility operating a classified system to conduct an examination of the adequacy of its practices and procedures to ensure that classified information is protected using multiple layers of cyber security protection, including protection against potential insider threats. Also, the memo required an accounting by each lab and facility for full implementation by January 15, 2007.

3. In response to findings contained within the Inspector General's report issued on November 27, the Secretary directed two actions. First, the creation of a senior level ad hoc committee to review all of the recommendations in the Inspector General's report except those concerning the Department's security clearance process. Second, the establishment of a task force to review the personnel security programs throughout the entire DOE complex. Both reviews will conclude and provide recommendations to the Secretary no later than February 28, 2007. Once we have reviewed the results of the Laboratory's actions, corporate and Federal validation activities, the Secretary's two Task Forces' recommendations, and other actions that have been directed, we will develop additional improvements and conduct follow-up reviews, as necessary. We will be pleased to discuss with the subcommittee the additional actions the Secretary decides to take once he has received and reviewed the Task Forces' recommendations.

4. Furthermore, during numerous occasions, meetings and conversations with the NNSA Administrator and his team, the LANL Director, and members of the Executive Board of LANS, LLC, the Secretary and I have expressed our depth of concern, sense of urgency, and expectations for accountability from the top of the department down to the bottom of the laboratory, and that these continuing security problems must be addressed, rectified, and prevented in the future.

5. Even before the recent incident at LANL, the Department had substantially increased focus and attention on matters of cyber security, including hiring a new CIO to reinvigorate and strengthen our efforts. Among other things, he accelerated the effort to update our cyber security order and National Security Systems Control Manual and has taken numerous actions to improve our Department-wide cyber security posture. We also brought in a new Chief of Counter-Intelligence and reorganized the office to improve its performance.

6. The Department also previously recognized that the leadership of the laboratory could be strengthened by competing the M&O contract. And last July, a new corporate leadership team took over management of the laboratory for the first time in its 64 year history.

7. Finally, because it is our view that we are accountable to the President, the Congress, and the American people not just for efforts, but for results, the Secretary and I made the difficult decision to replace the Administrator of the NNSA.

Only time will tell if we are to be successful. But the Secretary and I are committed to making the tough decisions required to lead our Department to a level of security performance befitting the great missions you have asked us to carry out. We have made progress in improving security across the Department and at Los Alamos, but as the latest incident indicates, we have much more work to do. We remain committed to the task.

I am happy to answer your questions at this time.

**Summary of the Statement of Dr. Linda Wilbanks**
**Chief Information Officer**
**National Nuclear Security Administration**
**U.S. Department of Energy**
**Before the**
**Committee on Energy & Commerce**
**Subcommittee on Oversight & Investigations**

**January 30, 2007**

Dr. Wilbanks' testimony will address the cyber security incident at the Los Alamos National Laboratory (LANL) and the actions the National Nuclear Security Administration (NNSA) has taken to prevent additional incidents.

It will include her responsibility within the NNSA Management Structure and background/qualifications of Dr. Wilbanks as the NNSA Chief Information Officer.

NNSA Cyber Security Program Manager and the Director of the Diskless Workstation Taskforce immediately flew to Los Alamos with two members of the Department of Energy's (DOE) cyber security team to identify the issues.

Actions taken as a result of the incident include:

- Requiring all NNSA sites to identify open ports on classified systems, and determine whether they needed to be open or could be permanently disabled. We purchased an enterprise license for software to monitor open port activity. All sites, including LANL, are now in compliance, will all ports that can be used to transmit data, sealed or monitored.
- The Designated Approving Authority (DAA) is responsible for approving an IT system for operations by signing the cyber security plan states how the system will be compliance with NNSA and DOE policy. We have temporarily reassigned the DAA from the Sandia Site Office to LASO to strengthen the Federal cyber security oversight and inspection capabilities. All DAAs are to review all system cyber security plans and hold them accountable to ensure they address the specific risks of each system and to identify and rewrite plans with omissions such as those found at LANL.
- NNSA Increased funding to the Los Alamos Site Office to hire three cyber security experts to support the DAA and cyber security activities such as updating plans and doing visual inspections to ensure compliance.
- NNSA assembled a team of eight cyber security experts from HQ and NNSA sites and have them inspecting all vaults at LANL to determine if they were in compliance with the Department's directive to close ports. The team initially found areas of noncompliance, however, when reconvened on site this past week, they inspected all 142 vaults and all are now in compliance with cyber security requirements.
- NNSA has have further directed the team to inspect the cyber security implementation at all NNSA sites. Those inspections will start in February and conclude in April when the team revisits Los Alamos.

**Statement of Dr. Linda Wilbanks**
**Chief Information Officer**
**National Nuclear Security Administration**
**U.S. Department of Energy**
**Before the**
**Committee on Energy & Commerce**
**Subcommittee on Oversight & Investigations**

**January 30, 2007**

Thank you for the opportunity to discuss the cyber security incident at the Los Alamos National Laboratory (LANL) and the actions the National Nuclear Security Administration (NNSA) has taken to prevent similar incidents at other NNSA sites. We have a very important national security mission and take these responsibilities very seriously.

Within the NNSA, the Chief Information Officer reports directly to Mr. Michael Kane, the Associate Administrator for Management and Administration. As the CIO, I am responsible for information technology within NNSA. I came to NNSA after almost three years as the CIO at Goddard Space Flight Center, NASA. I have over 30 years experience in information technology with a bachelors degree in Mathematics, a Masters degree in Engineering, and a Ph.D. in Computer Science. My office works with the Department of Energy (DOE) CIO, Mr. Tom Pyke, and the NNSA sites to develop and implement appropriate cyber security policies.

NNSA is dependent on information and upon the systems that create, process, store, and communicate information to carry out its national security mission. We must

guard against a wide range of attacks from the sophisticated outsider who wishes to break into our cyber infrastructure as well as the accidental or malicious insider. As the NNSA CIO, I am responsible to the NNSA Administrator for cyber security, specifically policies and procedures to ensure the security of the information and technology as it relates to the NNSA mission, and to enhance NNSA's ability to protect NNSA's classified, sensitive and unclassified information and systems.

I would like to provide the Members of the Committee additional information relative to actions the NNSA has taken in response to the recent LANL incident. I will then address actions specific to LANL and those actions taken across the complex.

When the most recent incident was reported, the NNSA Cyber Security Program Manager and the Director of the Diskless Workstation Taskforce immediately flew to Los Alamos with two members of the Department of Energy's (DOE) cyber security team. Their objective was to learn as much as possible about the incident from the cyber perspective and determine if any of the contributing factors could put LANL or other sites at risk. In November, I flew to Los Alamos myself and spoke with both Federal and contractor cyber security personnel, who are responsible for the computer systems at Los Alamos, including the system in question.

At Los Alamos we found was that there was a cyber security plan in place for the system signed by the Designated Approving Authority (DAA) who is located at the Federal Site Office. However, upon review following the incident, my office believed

that the plan was too generic and did not address specific risks to that system. For example, the plan stated that the cages containing the servers did not have to be locked as they were contained within a Vault Type Room and only authorized personnel were allowed in the room. The plan also allowed for scanning and for a printer to be connected to the classified systems even though there was no justified need to print. The server in question had accessible USB ports on the front and back that were not visible to the cyber security person in the room. These conditions allowed the subject in question to download classified data to her personal thumb drive. In order to move data to or from any of the servers, a password was needed. The subject in question only had the password to the server dedicated for scanning purposes, which was her assigned duty. This prevented her from accessing any information other than what she had been cleared to scan. We have since secured all USB ports at all NNSA sites and are reviewing all cyber security plans to ensure they address the specific risks for that system. This type of incident, the undetected transfer of classified information to a portable device, could no longer occur at any NNSA site.

We have undertaken a number of actions in response to the recent incident at LANL to prevent this type of incident and strengthen the cyber security:

- The DAA from the Sandia Site Office has been detailed to LANL to strengthen the Federal cyber security oversight and inspection capabilities.

- Additional funding was provided to the Site Office to hire three contractors to

support the DAA and cyber security activities. These contractors will be separate from the Laboratory contract.

- At the request of the Los Alamos Deputy Site Office Manager my office sent a team of seven cyber security experts from HQ and NNSA sites to inspect the vaults to determine if they were in compliance with the Department's directive to close ports. The on-the-ground team was able to verify that the lab was not in full compliance and because of that process we were able to initiate corrective measures. A team of federal cyber security experts went back to LANL on January 22 to re-evaluate the lab's efforts for compliance. The initial reports from this second team are positive and indicate LANL has corrected the deficiencies previously identified.

During the past year, NNSA has made changes to strengthen the cyber security posture of the complex and more recently addressed issues identified by the LANL incident.

- In early 2006 a Designated Approving Authority (DAA) official was appointed to work at each site. The DAA's sole responsibility is dedicated to cyber security for their site. Prior to this change one person was responsible for many systems at several sites. This resulted in cyber security plans that were more generic, that did not address specific risks and incorporated minimal, if any site inspections being done to verify the system was following the plan. A dedicated DAA at each site

will mitigate this vulnerability.

- Since a contributing factor to the incident at LANL was the generic cyber security plan, the Site DAAs that have now been assigned to all sites are currently reviewing all system cyber security plans to ensure these plans address the specific risks of each system. This review will identify plans that may be generic and allow peripherals that are not required (i.e., printers) or insufficient security, (i.e., unlocked cages) or any other omission or lack of specifics in the plan such as those identified in the LANL vault security plan. A standard template for a cyber security plan has been distributed to ensure all plans contain the critical information required to thoroughly asses the risks associated with operating an IT system. Each site is responsible for making the plan specific for each system, and removing weaknesses.

- In July, the NNSA Forensics Facility, Information Assurance Response Center (IARC) was assigned the responsibility for compiling all NNSA cyber security incidents and reporting them within the specified time periods to the Department's cyber security incident response center. All Sites, instead of having to report incidences to multiple places, now report them only to the IARC. This ensures the correct reporting of cyber security incidents and allows NNSA to track and analyze incidents, which will result in better risk identification and overall cyber management. This comprehensive information has already provided us with valuable lessons on areas that need to be strengthened across NNSA.

- In November 2006, as a result of the Los Alamos incident, we required all sites to identify all open ports on classified systems, and determine whether they needed to be open or could be permanently closed. We found that three sites had already identified this as a risk and were working on closure or had already closed the ports. (Deputy Secretary Clay Sell later issued a memo to implement this action for all of DOE by January 15, 2007.) We also purchased an enterprise license for software to monitor open port activity, an action that was in progress when the incident occurred. We have evidence that these actions are successfully working. On January 17, a personal thumb drive was inserted into a classified machine to upload work. The software successfully prevented the information from being uploaded to the classified machine and notified the system administrator.

- My office has worked with the DOE CIO, Mr. Pyke, to identify areas where policies and procedures are needed to strengthen cyber security guidance and to issue them in a timely manner. Those new policies included establishing a governance framework (Departmental Cyber Security Management) and establishing baseline cyber security controls for national security (classified) information systems (National Security System Controls Manual).

- We have set up a schedule for my office to inspect the cyber security implementation at all NNSA sites. Those inspections will start in February and conclude in April. Each inspection will last for one week. The inspection team will consist of two HQ cyber security personnel and a cyber security professional

from another site. These inspections will occur annually and strengthen Site office oversight. They will also serve as refresher training for the DAA on what they should be inspecting at their sites.

Cyber security programs are direct funded activities within Safeguards and Security line of the NNSA Weapons Activities appropriation. Funding allocation decisions are based on enterprise priorities and site risks. After my office identifies the risks and balances priorities for program initiatives, the Administrator takes the information into consideration with similar information from all other NNSA programs and makes overall resource allocation decisions across NNSA. In the current year, due to additional requirements placed on the sites in order to comply with the new policies and procedures, my office has reprioritized ongoing activities and reallocated $6M to cover these extra activities at the sites, of which $1.05M went to LANL.

NNSA is responsible for over 70 percent of the classified networks within the Department. We take this responsibility very seriously and have made maintaining the security of the classified networks our highest priority to ensure there are no breaches. The Department is on schedule with the implementation of diskless workstation project, and completion is scheduled for September 30, 2008. NNSA fully supports the Department of Energy's federated approach to cyber security that is directed in the recently updated Departmental order on Cyber Security Management, 205.1A. We are jointly working with the Department to maximize our efforts and resources to ensure a secure environment for the transmission and storage of our information.

Mr. Chairman, NNSA is working very diligently to maintain a secure environment for our information and that of the Department. We work closely with our sites to identify the risks and we work closely with DOE to maximize our resources. We are moving ahead in many areas and we are making progress.

# CONTINUING SECURITY CONCERNS AT LOS ALAMOS NATIONAL LABORATORY

**FRIDAY, APRIL 20, 2007**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
*Washington, DC.*

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2123 of the Rayburn House Office Building, Hon. Bart Stupak (chairman of the subcommittee) presiding.

Members present: Representatives DeGette, Green, Doyle, Inslee, Dingell [ex officio], Udall, Whitfield, Walden, Murphy, Burgess, Barton [ex officio], and Wilson.

Staff present: Chris Knauer, Richard Miller, Scott Schloegel, Rachel Bleshman, Lauren Bloomberg, Jodi Seth, Bud Albright, Alan Slobodin, Dwight Cates, and Matt Johnson.

## 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 on DOE's response to ongoing mismanagement at the Los Alamos National Labs. Each member will be recognized for 5 minutes for their opening statement, and I will begin.

Los Alamos National Laboratories is home to many of our Nation's most secretive weapons program, yet it is also home to some of the worst security breaches in our Nation's history. This is our 13th hearing on security problems at Los Alamos in just the past 8 years.

For 63 years, the University of California operated Los Alamos; but after numerous high-profile security lapses, the Department of Energy was urged to competitively bid the contract for operation of LANL. In June of last year, University of California was again awarded the contract under a limited liability consortium known as Los Alamos National Security, or LANS. This committee anxiously awaits proof that this new contractor will result in significant changes in Los Alamos and not just put new drapes over a broken window.

At our January 30 hearing, we investigated the October 2006 case of classified documents that were removed from Los Alamos by a contractor. We learned at that hearing that the security lapse would probably have not been discovered if it had not been for a domestic disturbance at the contract employee's home. The resulting investigation led to the discovery of drug paraphernalia and the discovery of classified paper and electronic files at the residence.

The female contract employee was not adequately watched by her escort. The employee also had access to open ports on classified computers which enabled her to download and remove classified documents.

We heard the Department of Energy's Inspector General testify in January that they do not know how much other classified information may have been removed using this gaping hole in security. We don't know where this classified material has ended up. We hope to learn the answers to these questions from the FBI's investigation, but they will not brief members until their investigation is complete.

Many of the members of this committee were shocked that the National Nuclear Security Administration, NNSA, approved a security clearance for this employee, even though she admitted using illegal drugs within 30 days of her security clearance being approved. We were equally shocked at the fact that there was no follow-up evaluation or testing of this individual after she was granted her security clearance. Apparently, her promise not to use drugs in the future was good enough for NNSA.

This security breakdown took place against a backdrop of previously degraded security performance. In 2006, the Department of Energy, Office of Health, Safety, and Security, documented substantial substandard-to-failing performance in 14 of 17 key security areas at Los Alamos. You can see the 2006 report right over there. The poor grades were in categories such as classified matter, protections and control, cyber security, and emergency management. Performance in 2006 had sharply deteriorated since the previous review in 2002 which had cited serious problems. I will be placing into the records summaries of these oversight reports. You can see them up on the screen now.

[Slide shown.]

In today's hearing, I hope to focus on a number of issues including what is the Department of Energy's system to issue classified security clearances? What led DOE to grant security clearance to an individual who admitted using illegal drugs within 30 days of her clearance being issued? What lessons are learned from this security lapse? What steps have been taken to correct the security deficiencies in the Department of Energy and at Los Alamos so that we do not have to hold our 14th hearing later this year?

At the January 30 hearing, DOE testified that the Secretary convened two task forces, one to examine cyber security and a second task force to look at personnel security issues raised by the latest security breach. Today we will hear the results of these task force reports. A key finding by the personnel security task force was that at least two additional employees admitted to illegal drug use in the 30 days prior to security clearance approval. Eighteen other employees had similar information in this 12-month period between 2001 and 2002 thereby causing DOE to re-examine their security clearances.

We look forward to hearing what Secretary Bodman plans to do about this and other security problems his task force has uncovered. We also look forward to hearing how he plans to hold the contractors accountable.

The Department of Energy has various tools, including enforcement action and reducing award fees to hold its contractors accountable. Nonetheless, this committee was disturbed to learn just this week that the Department of Energy apparently forgot to put legal requirements in its contract with the lab operator, the Los Alamos National Security. These legal requirements would have obligated the contractor to comply with DOE's stringent safeguards and security order known as DOE Order 470. This omission was discovered after the October 2006 incident which leaves open the question of whether the Department of Energy contracting officer may have handed Los Alamos National Security, the partner here, a get-out-of-jail-free card if and when DOE attempts to bring in enforcement action for multiple security violations associated with the October 6th incident.

The committee wants to know when the Department of Energy learned of this contract omission. Was it before last hearing where DOE officials swore they had all the necessary tools to enforce this new security standard? If so, why weren't we informed of this problem? When was the committee going to be told about this issue and what plans has the Department made to fix it?

After our January hearing, I, along with my Republican colleagues, asked the Government Accountability Office to evaluate whether the security footprint at Los Alamos is simply too large to manage the classified information effectively. We also asked GAO to evaluate the possibility of consolidating and moving classified operations at Los Alamos to another lab such as Sandia where security is managed more effectively. GAO is moving forward on this evaluation despite requests by some legislators to do an analysis.

In addition, the committee is reviewing H.R. 703, legislation introduced on a bipartisan basis with my colleagues, Mr. Barton and Mr. Whitfield, to move responsibility for safety and security out of NNSA and place it under the direct control of Secretary of Energy. We would welcome hearing the Secretary's view on this legislation. Secretary Bodman and his predecessors have come before this committee with commitments to improve the security culture at Los Alamos. Despite the creation of security czars and task forces, the end result has been a litany of security breaches and mismanagement. To say the least, the committee is skeptical.

Today, Mr. Secretary, we want to know, what is different? Why are your proposals more likely to succeed when your predecessor's proposals have not? What assurances can DOE give us that these new reforms will work? What resources, and from whom, will DOE look to pay for these new security measures at Los Alamos? I can assure you, Secretary Bodman and the American public, that the committee will continue its oversight at Los Alamos. I can also assure you that this oversight will continue just as it has in the past in a truly bipartisan basis. When it comes to Los Alamos and security at nuclear labs, this committee is united in its oversight.

I appreciate the assistance and cooperation of my Republican colleagues led by my friend, Mr. Whitfield, and his able staff.

And with that, I would yield to the ranking member, my friend from Kentucky, Mr. Whitfield, for his opening statement, please.

**OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY**

Mr. WHITFIELD. Thank you, Chairman Stupak, and for today's hearing to review ongoing security mismanagement at Los Alamos.

Over the past decade, this subcommittee has established a rigorous tradition of strong, bipartisan oversight on DOE security matters, and I am pleased that this committee has continued this tradition with its close attention to ongoing mismanagement at Los Alamos.

The most recent security incident, which occurred last October, resulted in the loss of over 1,500 classified documents. As I pointed out at the January hearing, this incident demonstrates poor security management, lack of formality of operations, and insufficient oversight that has plagued the lab for decades. Dramatic new ideas from the Department, from LANS, and from Congress are needed.

At Los Alamos, the security environment is certainly challenging. Operations are spread out over a 43-square-mile area. The lab has approximately 15,000 employees. There are more than 2,000 classified computers and 1,774 separate security areas. To give perspective, there are more classified security areas at Los Alamos than there are total rooms in the Rayburn, Cannon, and Longworth House Office Buildings combined. Los Alamos has an unnecessarily large volume of classified information and conducts classified activities in too many areas involving too many people. These factors, including the geographical dispersions of activities, continue to make LANL susceptible to security failures.

At the last hearing, I stated that LANS must be held accountable for the loss of classified documents last October and that it should pay a price. The Department of Energy must assert its contract and regulatory authorities to compel greater security performance. The Department has three primary tools to help compel performance, the enforcement of new information security relations with strong, civil penalties; the withholding of incentive pay associated with security performance; and three, the use of the conditional payment of fee clause in the contract that allows the Department to withhold up to 100 percent of the award fee.

The Department has not yet finalized how they will use these enforcement tools, but I know members of the committee and in the Congress will be quite interested in what the final decision will be.

Six months have elapsed since the October 2006 security incident. That is a reasonable amount of time to allow NNSA and LANS to formulate a plan to help improve security at the site. Later today, we will hear from Lab Director Michael Anastasio on the remedial actions he has taken to correct security failures. I think Director Anastasio's efforts to date appear to be more responsive than what we've seen in the past. I am encouraged by his initial steps to reduce the number of classified vaults at Los Alamos, and I think LANS has already implemented a few valuable cyber security improvements at the site. However, it is too soon to say whether these actions are simply short-term fixes or a commitment to long-term security improvements. I am delighted Secretary Bodman has joined us today, and we certainly look forward to his

views on this very important issue. And thank you, Mr. Chairman. I yield back my 1 minute.

Mr. STUPAK. Thank you, Mr. Whitfield. Next, turn to the Chairman of the full committee, Mr. Dingell, for an opening statement, please.

The CHAIRMAN. Mr. Chairman, I thank you, and I commend you for holding this hearing. Mr. Secretary, welcome.

Secretary BODMAN. Thank you.

The CHAIRMAN. I hope your visit here is pleasant here today.

Secretary BODMAN. So do I.

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

The CHAIRMAN. Mr. Secretary and my colleagues, today's topic is sort of as what is observed as deja vu all over again. The security at the Energy Department labs, in particular the one we are discussing today, Los Alamos National Laboratory, is an issue with which this committee has been involved for more than two decades. Our colleagues on this committee and I could produce stacks of letters and piles of hearing documents relative to the question of security breakdowns at the Department of Energy and at this unfortunate laboratory in particular. Likewise, we could display a small mountain of proposals and promises made by lab directors, blue-ribbon panels, task forces, Secretaries of Energy, and yes, even a few Presidents to fix the security problems at the labs.

You, Mr. Secretary, are no different than your predecessors, and you inherited a fine mess out there. You have proposed a number of changes and recommendations to fix the problems, and we commend you for that; and you've convened blue-ribbon task forces to make these recommendations. For that we are appreciative. I am sure that we will hear about how everyone takes this matter of security seriously. I am sure that in fact everyone is sincere about improving security; and I am certain that you, Mr. Secretary, will propose changes that will make sense.

But before we claim victory in our battle to improve Los Alamos, we need to look closely at what is being proposed and whether in fact it differs from what has happened before or what has come before. As President Reagan used to say, trust but verify. As my old daddy used to tell me, trust everybody but cut the cards. I would urge my colleagues to do that today. In this regard, I recommend you pay particular attention to the tools that you, Mr. Secretary of DOE, actually have to enforce the new security proposals.

I understand that the Department's ability to assess an effective fine has come into question in the light of information provided to the committee this week. The DOE officials who reviewed and signed the contract on behalf of the U.S. Government were the new contractors, Los Alamos National Security, apparently omitted the applicable safeguards and security orders for 13 months. This is hardly an auspicious way to start new reforms. Although legal implications of this omission are still unclear, it appears there is a serious question as to whether DOE is unable to cite the contractor for each and every violation of its security requirements. Apparently, applicable security requirements under DOE Order 470 were

not inserted into the contract until after the violations were discovered. In fact, these requirements were not included in the contract until after January 25, 2007, a mere 5 days before our last hearing on Los Alamos. I am curious to know why this information was withheld from the committee until now. This is certainly not trusting and verifying.

I hope the Secretary abides by this maxim, too. Mr. Secretary, do not trust everything that you are told. I would observe that we have been working on Los Alamos for a long time, and our problems with security there have been substantial and have run all the way from penetrations by foreign countries into the security there to loss of valuable Government property to problems with regard to stings that were supposed to be held to address problems of narcotics sales inside the facility and, very frankly, also two other things including a curious event involving fornication in the guard towers out there.

Mr. Secretary, I note with both respect and affection that you are not only requiring briefings from your staff regarding security and safety issues when you were there but that you also poked around the basements and nooks and crannies to assure that the situation with regard to security was going properly. Certainly, Mr. Secretary, we need that kind of approach today. I think we have to look beyond fines and penalties to fix the problems at Los Alamos. For that reason, along with my good friend, the chairman of the subcommittee, our good friends and colleagues in the minority, we have requested that the Government Accountability Office, GAO, conduct a comprehensive audit of Los Alamos to determine what functions are essential at that laboratory. Their report will inform us of the options available.

Mr. Secretary, I hope that you will assist the committee and the GAO in this important study and in our efforts to improve security at Los Alamos and throughout your Department. I thank you for your presence here. I express to you my affection and respect and also the hope that you will have success in straightening up something which has defied your predecessors in office in this matter.

I want to thank all of our witnesses for appearing before us today; and you, Mr. Chairman Stupak, I want to express my particular respect and gratitude to you for what you are doing. Thank you, Mr. Chairman.

Mr. STUPAK. Thank you, Mr. Dingell. Next we go to Mr. Walden from Oregon for opening statement, please.

**OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON**

Mr. WALDEN. Thank you very much, Mr. Chairman. And I, too, appreciate the continuing efforts in a bipartisan manner of this subcommittee to try to figure out how to provide full security at these labs. And Secretary, I want to welcome you as my colleagues have done and appreciate the work you're doing on this.

I noted in your testimony that you indicate that you feel like that significant progress has been made in security at Los Alamos and yet then you go on to say you're still not satisfied. I would be curious to know with only 20 months left in office, provided you're there to the end, how are we going to get this thing resolved and

do you think it is possible? We have had, as you know, multiple hearings over multiple years in both classified settings and nonclassified settings and continue to chase this. And if anybody can get this fixed, I have confidence that you certainly have the commitment and the ability to get it done. So I will look forward to hearing that. Before I have held up the J. B. Weld which is the world's finest cold glue I guess for households and hobbies. It is great for farm machinery and equipment. It is also $4.99 at Wal-Mart and was used I believe to plug something in the order of 7,200 USB ports at Los Alamos but only after there had been about a year of security breach. It seems to me that for $4.99 you can fix this problem. Maybe it wouldn't cost that much more to fix the whole thing. But it has been very disturbing that data can come and go in and out of the lab, and the most recent examples are very frustrating for us and I am sure for you, Mr. Secretary.

So we welcome you here today. We look forward to hearing your comments, and unfortunately they tell us we are going to have a long series of votes beginning in about 9 minutes. So I am going to quit and return the balance of my time and look forward to your comments. Thank you, sir.

Secretary BODMAN. Thank you, sir.

Mr. STUPAK. Thank you. Mr. Green from Texas, opening statement?

Mr. GREEN. Mr. Chairman, I'll just welcome the Secretary and submit an opening statement for the record.

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

Mr. Chairman thank you for calling this hearing.

I would also like to thank our witnesses, including Secretary Bodman and Los Alamos Director Anastasio for returning here a couple months after our last hearing to provide us with a status report on ongoing security measures at Los Alamos National Lab.

Given the situation at the national laboratory system, congressional oversight is a necessity.

Security can be high tech, involving counter-measures for computer hackers and electronic warfare, or it can be very low-tech, such as old-fashioned human intelligence.

The national laboratories, particularly Los Alamos, have had problems with both issues, as we see in the reports on Personnel Security and Cyber Security that the Inspector General has produced.

On the personnel front, this committee is going to be very interested in the ongoing review of security clearances and background checks for all employees in the DOE national security complex.

We are pleased to see a full review over issues like drug history and the implementation of new drug testing measures.

In addition, we need to ensure the security clearance review is not only looking at narcotics, since there can be many other security risks as well.

If people working on sensitive national security projects have any kind of major criminal activity or other issues that could make them a security risk, then DOE needs to know about that.

Often the lab has taken a reactive security approach, going from one crisis to another trying to prevent the same thing from happening again.

We need a proactive approach that thinks ahead to what other kinds of security breaches COULD happen, but haven't happened yet.

On the cyber security front, our committee is looking for a full update on issues like sealing open USB ports in lab computers, disabling dual use computer ports, and securing racks of computers with sensitive national security information.

Personnel security and cyber security are related, because sometimes it is just as important to know who is on the computer system as it is to know who is actually handling bomb-grade radioactive materials.

Mr. Chairman, with that I would like to yield back so that we may get to the question time for the witnesses. Thank you.

Mr. STUPAK. Mrs. Blackburn from Tennessee.

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

Mrs. BLACKBURN. Thank you, Mr. Chairman. I do want to thank you for holding the hearing and thank you and our ranking member, Mr. Whitfield, for the work on the issue; and I want to thank our participants for being here on what looks like is going to be an interrupted day. And before we begin the hearing, I do want to give a little bit of an overview of how I see things and how I think a lot of people that are looking at this with us see things.

It seems that, and we all know and it is frustrating, there is a systemic problem with management at Los Alamos, and for several years the culture of—has seemed to persist. It has gone on without seeming to have a lot done about it, and I see no significant efforts by NNSA or the DOE to change the culture; and I come to this decision by reading the reports that you have given us. I am partially relieved to see that the previous organization which appeared to be incompetent in so many different areas, that they have been replaced; and I have several concerns about the new operator and we will address those in questions. And from time to time, I think we see new policies that are brought forward; and Mr. Secretary, we hold great hope for you that new policies this time are actually going to do something to correct the problem, that there will be timelines, that there will be guidelines and some accountability measures that are there. I think all too often we see that people admit there is a problem, they find the problem; but unfortunately, they do not seem to have the desire to correct the problems, and that is the situation in which we find ourselves right now. Not correcting the problems it appears to me to each employee would be a disservice to their personal record, it would be a disservice to the administration, it is definitely a disservice to the American people. It is something that I hope we hear from the director and also from you, Mr. Secretary, that it is no longer going to be tolerated and that you can give us some measureables and some quantitative data that will prove to us that changes are indeed taking place.

We are hopeful for your progress, and I yield the balance of my time.

Mr. STUPAK. I thank the gentlewoman. We will next move to the gentlewoman from Colorado, Ms. DeGette.

**OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO**

Ms. DEGETTE. Thank you very much, Mr. Chairman. We were trying to count the number of these Los Alamos hearings that——

Mr. STUPAK. Thirteen.

Ms. DEGETTE. Thirteen? And those are all the ones we have been sitting in together plus the visit down there. Secretary Bodman, I am delighted to see you today; and I am really glad you came because I think that resolving these problems is going to have to

come from your level, and I know you have got that commitment. So I am pleased.

I am going to submit my whole statement for the record because frankly I am really tired of saying the same thing over and over again and emoting about what a disaster it is down there, and this latest incident with the employee who apparently had problems with her security credentials and then she takes critical documents on a flash drive and then she gets busted for drugs, it just boggles the mind. And it goes on and on.

But there are some really important legal questions that we have heard about in recent days that add yet a new dimension that I haven't even whined about once because they just came to light and that is about the contracting procedures at the Department of Energy. The committee has learned that the management contract signed by the Department and with great fanfare I may add lacked key components that allow penalties to be assessed when DOE security procedures are not followed; and because those orders were inadvertently omitted from the contract, so have the security breaches we have seen could go unpunished which frankly just underscores the cavalier attitude really that a lot of people take toward security at what should be frankly our most secure facility.

So here is the big picture. The American people need to know that management at Los Alamos, which comes from a lucrative, multi-million dollar contract, is top notch. That hasn't been the case, far from it. And all of our constituents need to have the confidence that if managerial negligence is found, if security breaches do occur, and if specific DOE procedures are not followed, then there will be severe consequences. That hasn't been the case, either. Enforcement so far has amounted to a slap on the wrist, and I think we all agree that is not acceptable. So there will be several questions I will be exploring today, what went wrong with the contracting procedures at DOE, how could these omissions have occurred, has this compromised the Department's ability to enforce its rules and assess penalties, and what is being done to ensure that this does not happen again?

Thank you, Mr. Chairman. I look forward to this hearing, and I am sure there will be many more. I yield back.

[The prepared statement of Ms. DeGette follows:]

**Rep. Diana DeGette**
**Opening Statement**

**The Department of Energy's Response to Ongoing Mismanagement at the Los Alamos National Labs**

**Subcommittee on Oversight and Investigations**
**Committee on Energy & Commerce**
**April 20, 2007**

**Thank you, Mr. Chairman. I appreciate your continued diligence in scheduling hearings on this issue. This committee has an important oversight role over the Department of Energy and specifically the Los Alamos National Lab.**

**It's good to see you again, Secretary Bodman. Thank you for your willingness to appear this morning. I am also pleased to welcome back Inspector General Friedman and Mr. Michael Anastasio, the director of Los Alamos National Labs.**

**In January, I was shocked to learn about the latest security breaches at Los Alamos. That a young staffer lacking proper security credentials was able to leave the facility with critical documents on a flash drive is unacceptable. Sadly after eight years of hearings, it is apparent that this is not an isolated**

**incident but but rather a systemic lack of management and proper security precautions.**

**Since our last hearing, more information has come to light, specifically about the questionable personnel security procedures and cyber security (or lack thereof) at the facility.**

**I hope to learn today if the hiring practices and security screening of applicants is appropriate for a facility that provides stewardship of our nation's nuclear weapons stockpile.**

**Cyber security is a growing threat, and I am tired of being told by witness after witness that the problems are being fixed when they clearly are not. The Department and the lab management need to transform security systems so they are not constantly reacting to the latest security breach, but being proactive.**

**I look forward to hearing about what the DOE has found in its recent investigations into these two important issues.**

**Finally, there are some important legal questions that have arisen in recent days about the contracting procedures at the**

**Department of Energy. This committee has learned that the management contract signed by the Department, (with great fanfare, I might add) lacked key components that allow penalties to be assessed when DOE security procedures are not followed. Because these orders were inadvertently omitted from the contract, some of the security breaches we have seen could go unpunished.**

**Mr. Secretary, I hope today you can shed some light on this murky legal question.**

**Here's the big picture: the American people need to know that management at Los Alamos, which comes with a lucrative, multimillion dollar contract, is top notch. That simply hasn't been the case; far from it. And my constituents should have the confidence that if managerial negligence is found, if security breaches occur, if specific DOE procedures are not followed, that there will be consequences. That hasn't been the case either. Enforcement thus far has amounted to a slap on the wrist, and that's not acceptable.**

**There are several questions I will be asking today. What went wrong with the contracting procedures at the DOE? How**

**could these omissions have occurred? Has this compromised the Department's ability to enforce its rules and assess penalties? What is being done to ensure this doesn't happen again?**

**Thank you again, Mr. Chairman. While I look forward to this dialogue today, I hope we're nearing the end this committee's investigations of Los Alamos.**

Mr. STUPAK. I hope not but I am afraid there will be. Mr. Murphy, opening statement, please.

Mr. MURPHY. Thank you, Mr. Chairman. I will waive in interest of time, but I would like to welcome the Secretary for being here. Thank you.

Mr. STUPAK. Thank you. Mr. Doyle from Pennsylvania, opening statement, please?

**OPENING STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA**

Mr. DOYLE. Thank you, Mr. Chairman. I want to commend you for your continued vigilance on this important matter.

The protection of classified documents and information at our national labs, especially at Los Alamos National Lab, is critical to ensuring that we are able to protect the American public against those who may intend to do us harm. The frequent security breaches at this and other labs are completely unacceptable. I am looking forward to hearing the testimony of Secretary Bodman and his colleagues as we work together to ensure our nation's classified nuclear information remains protected.

It is no secret that there are and have been over a number of years serious security questions at the Los Alamos National Lab. Thankfully, most of these breaches have been of an accidental nature due to inadequate security breaches being in place. In essence, the breaches have served as a wake-up call to all of us. I shudder to think what may have occurred had the breaches been the result of a well-thought-out and intentional plan to secure classified information for sale on the black market. We have been lucky so far. But if security there is not made ironclad, our luck will surely run out.

I am looking forward to hearing about the improvements that have been made since October 2006 investigation, as well as what improvements have been made since our last hearing on this matter in January. I am so very interested in being able to judge the level of commitment to security improvements, not only on the ground at the site but all the way to the Secretary's office. I believe it is critical that the Secretary maintains his vigilance, not only on this particular incident but on the entire security systems under his prevue.

One thing is clear, when it comes to the long history of violations at Los Alamos, an intensive, short-term focus which trails off once the media focuses on another subject, will only lead to future concerns at the lab. We on this committee, those in the administration, and those on the ground at the labs must continue to shine a light on security while working together to ensure that procedures are updated so that the facilities are not only more secure today but will become even more secure with the passage of time.

Former Secretaries of Energy have come before Congress with promises of new security; but for one reason or another, they have fallen short and violations have continued. Now this matter falls to you, Secretary Bodman. We on this committee hope to work closely with you so that you will succeed where your predecessors have failed. Security, especially nuclear security, is not a Democratic or Republican issue, it is an American issue in which all branches of

Government and both political parties must work hand in hand to ensure that the American people have the protections in place they deserve. We must renew this focus today and continue to fully and completely protect our facilities and the critical information they possess at both the physical and cyber levels. Anything less opens our nation to dangers that none of us even want to believe could happen.

So again, Mr. Chairman, I commend you for your continued vigilance. I will look forward to hearing the testimony of our distinguished panelists, and I yield back the balance of my time.

Mr. STUPAK. Mr. Burgess.

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

Mr. BURGESS. Thank you, Mr. Chairman. I guess I am glad we are here today. Like everyone else, I am frustrated that we never seem to make any forward motion on this. It is a bipartisan issue. We all share the same concern and anxiety regarding security at the lab. I appreciate the aggressive nature the committee has taken on the crucial issue of national security.

We have three witnesses today that can provide insight into the problems and hopefully solutions to the Los Alamos problems. Secretary Bodman, Inspector Friedman, Director Anastasio, gentlemen, I welcome you all here today and I look forward to entering into a constructive discussion with each of you. I understand that there have been improvements made, but there are still many, many challenges ahead of both you and us.

Today we are going to be reviewing the findings of both the personnel security task force and the cyber security task force. I am encouraged by reading about the task forces, but unfortunately, we have been told in the past that actions and repercussions will occur but they never do. That is why we have held hearing after hearing, year after year, on Los Alamos. To quote the Inspector General in his written statement, "Many of the actions are in process and the key to the successful resolution of the matter is detailed in our November report, its implementation and execution." Implementation and execution. You all have good ideas that will significantly affect the security of Los Alamos, but it is not enough for us to come here and hold these hearings and talk and talk and talk about it. One of these days someone is going to have to walk the walk. I am still not completely comfortable with using basically the same contractor for operating Los Alamos. I do believe that Director Anastasio was capable and qualified to help turn things around but also mentioned during the last hearing, you have some of the most intelligent minds in the world at work at Los Alamos. While there is clearly an institutional problem, we must also remember that there are thousands of hard-working employees at the lab who make a remarkable contribution to science and the country on a daily basis.

Also at the last hearing, we discussed the issue of accountability. It is appropriate to readdress that issue today. While there are many organizational changes that can be made to better ensure the security of our country's classified information, one of the easiest and most effective remedies is to make the contractor in charge of

security pay a steep and deep penalty. As a steward of the taxpayer dollar, I fully support this idea. If the contractor is penalized substantial sums, and in Washington substantial sums are substantial sums of dollars, maybe then they will finally recognize how serious of a problem this is and must be stopped at all costs.

One of the other things we learned at our hearing earlier this year was the fact that although the contract for the lab had been rebid and re-awarded, that that process could be opened again if there were substantial problems encountered. I would submit to you that it appears that there are substantial problems, but I would like an update on whether or not the Department of Energy is going to hold the contractor accountable for his actions or lack thereof, if there is going to be a reopening of the contract that was awarded the past year.

I have also another issue within the Department of Energy that I think is appropriate to briefly mention and discuss. I understand that there is a strike occurring at a nuclear security weapons plant in my home State of Texas, the Pantex facility, and I would appreciate it if Secretary Bodman would give us a brief update on that issue and the impact of security at the plant.

Again, Mr. Chairman, thank you for holding this bipartisan hearing in which we can further address the security at Los Alamos. We are all committed to continuing these hearings until this cycle of security breaches at Los Alamos is over once and for all.

I yield back.

Mr. STUPAK. That concludes the opening statements. For the record, Mrs. Wilson is here from New Mexico and so is Mr. Udall, not members of the subcommittee but we welcome you, and I know you have been at every hearing we have had on this, Tom; and you certainly can be here when we go to the questions, and we will certainly give you an opportunity to ask questions if you like.

So that concludes the opening statements by members of the subcommittee. I will now call our first witness to come forward. Our first panel we have The Honorable Sam Bodman, Secretary of the U.S. Department of Energy. Secretary Bodman, it is the policy of the 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 during the testimony. Do you wish to be represented by counsel?

Secretary BODMAN. No, sir.

Mr. STUPAK. OK.

[Witness sworn.]

Mr. STUPAK. Mr. Secretary, you are under oath. You may begin your opening statement, please.

**STATEMENT OF HON. SAMUEL W. BODMAN, SECRETARY, DEPARTMENT OF ENERGY, WASHINGTON, DC**

Secretary BODMAN. Mr. Chairman, Ranking Member Whitfield, members of the subcommittee, I am very pleased to be here to discuss what I consider to be one of the most pressing management issues confronting my Department.

Since coming to the Department, one of my top goals has been to institute a safer, more secure work environment across the DOE complex, and I have meant this to include physical safety and secu-

rity as well as cyber security. I want to be absolutely clear with all of you, the protection of sensitive information is essential to our ability to meet the mission of this Department. Without it, we can't do it.

What I would like to do today is to briefly outline the steps that we have taken since the Deputy Secretary testified before you in January. In summary, I would make two points. First, we have made significant progress in my judgment, and I am confident that we are on the right track. That being said, we are not satisfied with where we find ourselves today. We are sitting on top of this issue, we continue to look for ways to identify and correct any potential weaknesses. If I may, I would like to now describe some of the improvements and also note that more details appear in my written testimony which will be submitted for the record, if that is acceptable to the Chairman.

First, we have made some senior management and oversight changes in response to the security breaches at Los Alamos. In January, I made what for me has been a very difficult decision and that is to replace the Under Secretary for Nuclear Security. Tom D'Agostino is the Acting Under Secretary and NNSA Administrator. In addition, NNSA has reassigned the Los Alamos site office manager and has put one of its strongest managers, Daniel Glenn, in place as the Acting Manager.

Further, Tom D'Agostino has requested that DOE's Office of Health, Safety, and Security conduct annual inspections at Los Alamos for the next 3 years. This month, both NNSA's Office of Defense Nuclear Security and CIO will inspect LANL for cyber and physical security problems. In fact, the CIO has already been there and conducted her inspection. The site office will conduct annual and regular observations of the laboratory's security program.

I would just add that I continue to be in close contact with the senior leadership of the laboratory. In fact, I met with all of the national laboratory directors just last week in Chicago. At a department level, I have formed two teams of senior officials, including Under Secretaries, the Chief of Security, and our Chief Information Officer and asked them to make specific recommendations based on the report of the Department's Inspector General who conducted his report at my request. I have directed that these recommendations be implemented department-wide, including enhanced mandatory training for those involved in granting of security clearances; a strengthened departmental policy on drug testing that hold security clearances, everyone; better quality assurance oversight for granting security clearances; and a revised organizational structure for our personnel security program that will ensure accountability.

We are also taking actions based on the recommendations from our cyber security team. Those include mandatory separation of duties for critical positions, improved training for all individuals with cyber security responsibilities, and improved line management oversight. We are carrying out the Department's new authorities related to assessing civil penalties for classified information security violations. At the same time, the laboratory's current management contractor, LANS, is also taking corrective action of their own. Among other issues, LANS recognizes that the lab's volume

of classified holdings is unnecessarily large, it is conducting in too many security areas, involves too many people, and is too spread out. As a result and with the approval of NNSA, they are aggressively reducing the number of locations where they hold and process classified matter.

In closing, Mr. Chairman, let me say this. The men and women who work at our national laboratories are among the world's most talented scientists and engineers. Since their founding, these laboratories have demonstrated again and again the tremendous power and terrific promise of science to help our nation solve our greatest challenges. But such a system cannot tolerate the kind of lapses in security that we have seen, be they in the physical or cyber realm. Protecting critical information and maintaining a vibrant collaborative science culture are not in my judgment mutually exclusive. Quite the opposite is true. In this case, you absolutely cannot achieve one without the other; and you continue to have my word that I will do everything in my power to support both objectives. The American people deserve no less.

I would like to say, sir, that in my view, the objectives of this committee and all of the statements that I have heard made by the members of the committee are very consistent with my own feelings. We have a real problem here, and I think we have the opportunity of working together to try to deal with it. Thank you very much.

[The prepared statement Secretary Bodman appears at the conclusion of the hearing.]

Mr. WHITFIELD. Mr. Chairman, may I ask a procedural question before we begin our questioning? I know that we do have some information, Official Use Only information, particularly relating to the rating summary for the Los Alamos plant and various areas, and in the past, whenever we've discussed Official Use Only information, we have either gone into executive session or a closed session or we have worked with the Department to agree on redacted material before we release anything to the public. I mean, that is one of the documents there. I know it has been partially redacted, but I would ask the chairman what his intent is on this issue relating to Official Use Only.

Mr. STUPAK. Well, I thank the gentleman for posing the question. As you can see on the ratings summary, and we had it up during my opening statement, that was the most recent Los Alamos site office and lab rating summary. The broad categories are there, but the detailed areas of security have been redacted at the request of the minority and the majority; and the documents with more detailed information in there will not be released and have no intentions of being released, even the ones I think we have in Secretary Bodman's book up there is all redacted. For the audience, the yellow part there is probably about a C-minus if we are grading this. Green is maybe a B. That's good. R is really bad. I guess that is what R stands for, really bad. In 1999, the report was better than this and we seem to be on a downhill slope. So I am sure there will be questions about it, but there are no details in there. What does emergency management, that is the broad category or cyber security, but we do not have any details in there nor do we intend to release any of those details. As you have said, they are for official

use, even though this committee or any member would have a right to release it I believe in a hearing in the context of their official duties, but we are going to leave it like it is.

Mr. WHITFIELD. Well, I appreciate——

Mr. STUPAK. Not to hold you up.

Mr. WHITFIELD. Yes, I appreciate that, Mr. Chairman. And I think all of us would stipulate that the grades that the Department has received on this are not particularly good, but I really appreciate your conveying that information. And I am assuming that is the only Official Use document that we have. So thank you very much.

Mr. STUPAK. If it would have had the details in, it would have been Official Use. Since it has been redacted, it is my understanding it is no longer Official Use. That document can be released. The ones that say Official Use with the details, there is no intention that I know of of anyone on this committee or myself or staffs of releasing that. Thank you.

In order to proceed in a more orderly and efficient manner, I would like to propose and set up 5 minutes for each member for questions, that each member will have 10 minutes to use for questioning during this hearing. Any objection? I see ranking member of the full committee, Mr. Barton, has just arrived. Before we go into questions, would you care to make an opening statement, sir?

Mr. BARTON. Thank you, Mr. Chairman, but I am a little bit late so to expedite the hearing, I know we have got some votes, so I will put my statement in the record.

Mr. STUPAK. Yes, we have nine votes coming up here. I don't know if you want to do an opening before we do the votes and I don't know if we want to get halfway through the questions and have to stop.

Mr. BARTON. No.

Mr. STUPAK. OK. Then we will proceed to questions. I will start off.

Mr. Secretary, the Cyber Security Task Force calls for an independent oversight review of cyber security at Los Alamos this year. Your testimony calls for annual reviews. Is Los Alamos in compliance with all DOE directives regarding security as we sit here today?

Secretary BODMAN. No.

Mr. STUPAK. In what areas are they still deficient?

Secretary BODMAN. Well, we have a number of recommendations that have been put in place in the cyber security area, most notably a systems manual that was delivered and made available to the contractors and with the stipulation that these be entered into the agreements with each contract.

Mr. STUPAK. So it is not entered into the contract?

Secretary BODMAN. They are in the process of being entered into it. I think it was on the date of March 8 that the security manual was issued. They have 90 days in which to accomplish that, and we expect them to accomplish that by June 8. Now that will then put it in being a part of the contract.

Mr. STUPAK. Correct.

Secretary BODMAN. There will then be a period of time. I can read through the various issues if you would like.

Mr. STUPAK. When do you think the implementation will be?

Secretary BODMAN. It is going to be a couple of years, sir, before all of this is done because this calls for training, it calls for a change in the way we manage the entire cyber security responsibilities of the Department.

Mr. STUPAK. If it is going to be a couple of years, I think we will be having a 14th, 15th, and 16th hearing then. In summary, you were summing up and you said LANS, the new contractor who is in charge of this lab——

Secretary BODMAN. Yes.

Mr. STUPAK. You see them, might as well call them, 60 percent of LANS is University of California——

Secretary BODMAN. No, sir, it is not, sir.

Mr. STUPAK. OK.

Secretary BODMAN. Sir, it is not. The 60 percent is not California.

Mr. STUPAK. OK. LANS is now in charge.

Secretary BODMAN. That is correct.

Mr. STUPAK. Sixty-three years of U.C., now we got LANS.

Secretary BODMAN. That is correct.

Mr. STUPAK. OK. LANS, if I heard you correctly at the end, LANS agrees that Los Alamos is too large, too many people, and too spread out is what you said at the end, correct?

Secretary BODMAN. They believe that the use of classified information, that there are too many centers, we have too many classified retrievable electronic media that are being used, and there is a specific program that I am sure Director Anastasio will review with you for reducing those.

Mr. STUPAK. OK. As you know, we have asked the GAO to take a look at this.

Secretary BODMAN. Yes, sir.

Mr. STUPAK. Not just in the cyber security but the whole footprint out there because many of us feel the repeated security breaches at Los Alamos, because it is too large, too many people, too spread out, and when it takes years to implement policy, we do not feel real confident that the implementation and the policy will be completed in a timely manner and we will be back here again with more breaches. So if it going to take years to implement security agreements, that really bothers us.

Secretary BODMAN. Well, some of it, sir, depends on budgets. In other words, these will be costly, they will require the approval of this Congress in order to get sufficient funds to do what needs to be done.

Mr. STUPAK. So the taxpayers are going to pay for all these new security measures?

Secretary BODMAN. It will be perhaps shifted around from one part of the organization to another, so I am not saying there will be a total increase in the budget but I am saying there will be a funding for this that is required.

Mr. STUPAK. Well, I don't want to throw good money after bad, but we are a little concerned here when we learned this past week that the enforcement mechanism for LANS wasn't even in the contract. Now, 13 months later I guess it is inserted. So when I said

get-out-of-jail-free card, that is from the game Monopoly and this is real money, not paper money.

Secretary BODMAN. I understand that.

Mr. STUPAK. You have a monopoly when one entity you see has managed this lab for 63 years and still is part of LANS. And so we can't be giving out get-out-of-jail-free, using taxpayer money, and a management monopoly and we are back here all the time doing the same thing.

Let me ask you this question. The Inspector General's testimony said the Federal and contract managers need to manage the lab more aggressively and the Department and the lab must develop a regiment of compliance testing. However, it appears you are going in the opposite direction by using a pilot program at Los Alamos which is based on reduced Federal oversight and increased contractor self-assessment. Given the core weaknesses in security, safety, and the history of mismanagement, do you believe that reduced Federal oversight is appropriate model at this time especially when it is going to take near 3 or 4 years?

Secretary BODMAN. Of course not.

Mr. STUPAK. Then why would you propose a test pilot program at Los Alamos?

Secretary BODMAN. I don't understand what that is. I never heard of it.

Mr. STUPAK. You have no idea? OK. All right. Secretary, is it true that during the investigation of the security incident the Department learned the subcontractor employee had taken an unsecure cell phone into the vault at Los Alamos?

Secretary BODMAN. Yes, I heard that yesterday in preparation for this hearing that there was some allegation of that, but I do not know anything about that.

Mr. STUPAK. We heard that some time ago. From the January hearing to now, we heard about this. We heard about the enforcement part of the contract not being there, now we hear about a cell phone. What are we going to hear about next? I thought we had this thing.

Secretary BODMAN. Mr. Chairman, I will repeat for you, sir.

Mr. STUPAK. Sure.

Secretary BODMAN. I do have a record of truthfulness and integrity in handling management matters. I do have a record of some competence in handling management matters. Now, some of your statements, sir, in my judgment are not correct. They have the wrong premise.

And I have attempted to correct those as we have gone along.

Mr. STUPAK. What is not correct?

Secretary BODMAN. So I will tell you, sir, that we are committed, I am personally committed, to trying to improve the security situation at Los Alamos. I frankly find myself in a position of some embarrassment. Why? Because I did not personally ask the right questions in the early days of my tenure in this job, and the questions might have been something along the line have all past Declarations of Secretaries been included in the policy that has been included in the contracts between this Department or between the NNSA and the contractor? The answer is no, they have not been. And so there are many things. Why haven't we had a compulsory

drug testing program for all members who are cleared? We have not had. We will now to the extent that we are able to do it. And so I am just saying that there are number of things that have been done, and I am here to tell you that I am committed to trying to get it done but I also repeat I am somewhat embarrassed I didn't ask all the right questions in the beginning.

Mr. STUPAK. Let me ask you, the January 30 hearing, did the Department of Energy know that they didn't put the enforcement mechanisms, the DOE Order 470, in the LANS contract in January?

Secretary BODMAN. I don't know, sir.

Mr. STUPAK. All right.

Secretary BODMAN. I learned about it about that time.

Mr. STUPAK. About that time?

Secretary BODMAN. Yes, sir.

Mr. STUPAK. And no one told us about it until last week?

Secretary BODMAN. That was about the time we learned about it. I may have been a week or two earlier, but I just don't know.

Mr. STUPAK. Well, last week is a lot different from January 30. That is quite a bit of timeframe. What about the cell phone incident in the vault? You just learned about that, too?

Secretary BODMAN. I just learned that the allegation of the cell phone in the vault. I don't know of the truth. This is an investigation, sir, that is still ongoing; and I would remind you on that, and so I am unable to comment on anything specific that I have heard. But I just tell you with respect to any questions about the cell phone, I have not heard about it before.

Mr. STUPAK. Well, when is your investigation anticipated then to be done?

Secretary BODMAN. It is not my investigation, sir. This is something being handled by the FBI.

Mr. STUPAK. OK.

Secretary BODMAN. So I can't answer for them.

Mr. STUPAK. So after the FBI is done and after they brief this committee, are you going to come back up to this committee then and tell us the facts of the investigation as you know it?

Secretary BODMAN. We will report to you the facts.

Mr. STUPAK. Well, we would just as soon get them on the record so we don't have to have more hearings, but this information keep dribbling out is not good.

Mr. Secretary, let me ask you this. Was it a violation of DOE policy, I am talking about DOE policy now, to approve a security clearance for an employee who admits to using illegal drugs in the 30-day period prior to the approval of their security clearance?

Secretary BODMAN. I don't know if it was a violation of DOE policy, but it didn't make any sense to do that, sir.

Mr. STUPAK. OK. And in review, we have seen at least two other employees and 18 others who have what you call derogatory information in it who have received security clearance that probably based on derogatory information should not have received it or had used drugs within 30 days of receiving that clearance?

Secretary BODMAN. I don't know what those were. I can tell you that part of the recommendation on the improvements in the secu-

rity system for the Department involves a review of all of the clearances that were provided——

Mr. WALDEN. Mr. Chairman, can I ask a point of parliamentary inquiry? I thought you moved that we would reduce the amount of time for questions to 5 minutes?

Mr. STUPAK. Ten minutes we said.

Mr. WALDEN. Ten minutes? OK.

Mr. STUPAK. Go ahead, Mr. Secretary. I think where you are going is the question I was trying to ask. The Department is going to implement the task force's recommendation to review all 4,360 security clearances——

Secretary BODMAN. There are some 4,000 that we are in the process of doing, and I expect to have that done during the balance of this season. I would guess during the summertime.

Mr. STUPAK. Thank you, Mr. Secretary. Mr. Whitfield for questioning? We have 6 minutes left.

Mr. WHITFIELD. I am going to take 5 minutes and then come back when—Mr. Secretary, before you came to the Department of Energy, and I know you have other Government experience, but you certainly had a reputation in the private sector as being a strong executive. And when you look at this situation, you hear a lot of comparison about Lawrence Livermore and Los Alamos; and we know that the University of California has been involved in the management of both of them for many, many years, for about 63 years or so, and yet there doesn't seem to be the problems at Lawrence Livermore as there is at Los Alamos.

From your position as Secretary of Energy and experiences running business, as a strong executive, why do you feel that there has been so much problems at one of these labs but not the other?

Secretary BODMAN. That is sort of a speculation on my part. I guess I would cite for you, sir, there are significant differences between the two institutions as to where they are located, geographic location, and getting the right management. In San Francisco is a very different matter than getting the right people to move to Los Alamos and to take on that assignment. So that would be one comment.

Comment two, I think it goes back to the very history of the laboratory. There have been issues of security, if you read back the history of this, for 60 years and there has been a very challenging environment there because of the preeminence of science and less interest apparently at times in security responsibilities. The one you should really ask that question of is Mr. Anastasio who will testify next. And if I had to answer that question, he is the person I would ask.

Mr. WHITFIELD. OK.

Secretary BODMAN. He has been at both places.

Mr. WHITFIELD. Who at the Department was responsible for overseeing the contract letting that LANS recently won and the security requirements were omitted from that contract? Who in the Department was really responsible for negotiating that contract?

Secretary BODMAN. Ultimately, I am responsible, Mr. Whitfield for the contract. You then go down through Linton Brooks who was the Administrator and oversaw the activity that had that responsibility, Tom D'Agostino who oversaw it. A lot of things went on if

I may say at that point in time. I also would add, this is the world according to Sam and not anything else, I think that there will be ample opportunity whether or not there is the specific inclusion of specific arrangements in there for whatever penalties are deemed desirable by the enforcement actions to be implemented.

Mr. WHITFIELD. Some people feel like the University of California has been involved in the management of this plant for 63 years; and there was a strong argument that maybe we need to just change it completely, and I know they are still a part of LANS.

Secretary BODMAN. Right.

Mr. WHITFIELD. Was there any discussion of that at the Department about maybe just a complete culture change by changing the major——

Secretary BODMAN. Yes, there certainly was a discussion, and I think that first of all it is important to recognize that there are very specific Federal procurement rules that apply that involve a Source Selection Officer and a Source Evaluation Committee that provides information for the Source Selection Officer, and these are all career employees. And so it is something that is done in order to prevent political interference with the ultimate decision.

So I know there was a discussion of this general matter, but I would think that it is important to recognize that the team was recognized for the combined scientific excellence in the University of California and the management expertise of both Bechtel as well as BWXT and the Washington Group.

Mr. WHITFIELD. Right.

Secretary BODMAN. Now, this group I will tell you, I have personally dealt with this board on a one-on-one basis meeting with both the chairman and the vice-chairman of the Board since this event occurred, I think it is fair to say this event caught them by surprise just as to how serious this matter was and is. They immediately dispatched their own people—I am sure Dr. Anastasio will review that with you—in order to review the situation. They found a very glaring failure in cyber security programs, they said about their own programs, over and beyond anything we are doing in order to try and deal with this.

Mr. WHITFIELD. Well, Mr. Secretary thank you. We have about a minute left so I guess we need to get over and vote.

Mr. STUPAK. OK. So we have seven votes, so let us adjourn. We should be back 11:15 or so. We will adjourn the hearing until then. How is that with you, Mr. Secretary?

Secretary BODMAN. Whatever you say, sir. I will be happy to——

Mr. STUPAK. Well, you got to remember——

Secretary BODMAN. I got a limit as to how long I can stay the rest of the day.

Mr. STUPAK. Yes, and unfortunately they give us seven votes right now.

Secretary BODMAN. I understand that and I honor that. I want you to honor what time pressures I have, sir.

Mr. STUPAK. I understand.

Secretary BODMAN. Thank you.

Mr. STUPAK. Thank you. The subcommittee stands recessed until 11:15.

[Recess.]

Mr. STUPAK. A lot longer than we all thought. We thought we had seven votes and it ended up being nine plus motions to recommit.

Unfortunately, the Secretary, as he indicated, had a noon appointment that he had to make and so we dismissed him. We may call him back at some time in the future. But had he been here I would have asked him again about DOE's pilot oversight model at Los Alamos that he seemed to know nothing about. I would for the record like to read the general question I asked the Secretary about this pilot. My question was, Mr. Secretary, the Inspector General's testimony said the Federal and contract managers need to manage the lab more aggressively in the Department and the lab must develop a regiment of compliance testing. However, DOE is going in the opposite direction by using a pilot program at Los Alamos which is based on reduced Federal oversight and increased contractor self-assessment. Given the core weaknesses in security, safety, and the history of mismanagement, do you believe that reduced Federal oversight is the appropriate model at this time? If so, why? The Secretary claimed he did not know anything about this pilot. In fact, our staff has provided an official Department of Energy memorandum establishing this pilot specifically for Los Alamos.

It is also my understanding that this pilot is well-known by other key officials including the Inspector General who is rather critical of it. I intend to ask the Inspector General, our next panel here, (a), if they know about the pilot and, (b), what concerns does he have about it. But now perhaps more importantly, I intend to ask the IGY when this memo was signed by the former NNSA Chief, Ambassador Linton Brooks, the Secretary would apparently know nothing of it. I find that troubling unto itself, and we will ask the Secretary in writing the same questions.

We have had problems as you all know in the past with the head of the National Nuclear Security Administration not conveying key management information related to the Secretary. I wonder if this is yet another example.

So we can move to our second panel so we can get these questions out. I will now call our second panel of witnesses, the Honorable Gregory Friedman, Inspector General for the Department of Energy, and Mr. Michael Anastasio, Director of the Los Alamos Nuclear Laboratory.

It is the policy of this subcommittee, gentlemen, to take all testimony under oath. Please be advised witnesses have the right under the rules of the House to be advised by counsel during their testimony. Do any of you wish to be represented by counsel? Mr. Friedman?

Mr. FRIEDMAN. No.

Mr. ANASTASIO. No.

[Witnesses sworn.]

Mr. STUPAK. Thank you. The record should reflect the witnesses have replied in the affirmative. You are now under oath. Mr. Friedman, we will start with you. Five-minute opening statement, sir.

**STATEMENT OF HON. GREGORY H. FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY, WASHINGTON, DC**

Mr. FRIEDMAN. Mr. Chairman and members of the subcommittee, I am pleased to be here at your request to testify in the concerns expressed in your April 5 letter regarding operations at the Los Alamos National Laboratory.

In January 2007 I testified before this subcommittee on the special inquiry conducted by my office regarding the diversion of classified data from Los Alamos. Specifically at the request of the Secretary of Energy, we examined the efforts of the Department and its contractors to protect classified information and the steps that were taken to assure that only authorized individuals had access to such information. Our report on this matter was issued on November 27, 2007. The Office of Inspector General found the security environment at Los Alamos is inadequate despite the expenditure of millions of dollars by the National Nuclear Administration to upgrade various components of the laboratory's security apparatus. In particular to the cyber security control structure we found that certain computer ports had not been disabled, classified computer racks were not locked, and some individuals were inappropriately granted access to classified computers and equipment to which they were not entitled.

In many cases, laboratory management staff had not developed policies necessary to protect classified information, enforce existing safeguards, or provided the attention or emphasis necessary to ensure protective measures were adequate.

Some of the security policies were conflicting or applied inconsistently. We also found the laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and physical inspections. In short, our findings raise serious concerns about the laboratory's ability to protect both classified and sensitive information systems.

The OIG also reviewed certain aspects of the security clearance process in place for laboratory employees. We identified particular weaknesses associated with this program which were discussed in a closed-session of this subcommittee in January 2007.

After this incident was discovered, Department and laboratory management officials launched several efforts to identify and correct and control deficiencies that certainly contributed to an environment which classified information could be removed without authorization. In particular, the Deputy Secretary directed an immediate review of policies and practices related to computer ports at each of the Departments' facilities. Further, the Secretary established two high-level task forces to address our findings. The reports of the Secretary's task forces and a list of the proposed directive actions were provided to my office last week. Many of the corrective actions outlined by the two task forces are in progress. Implementation, deployment, and execution are key. If properly carried out, the corrective actions should improve classified operations at Los Alamos and could help prevent similar incidents at departmental facilities throughout the complex.

As I have testified on several occasions, the Department must do a better job addressing the recurring challenges it faces, and I have four or five specific suggestions. Number 1, with regard to the cur-

rent matter, the Department must ensure that all actions and recommendations outlined in the Task Force Reports are formalized into policy and adopted as practice throughout the Department. As part of that effort, these policies should be incorporated into all facility contracts.

Two, to achieve the recommended reforms, the Department must establish firm schedules with specific implementation timelines and performance metrics. No. 3 both Federal and contractor officials need to manage more aggressively. As part of that process, the Department needs to ensure that its Federal contract management function is adequately staffed with the appropriate skill mix. In addition, Department and laboratory officials must develop a more comprehensive regimen of compliance testing and follow up to ensure that security policies and procedures are rigorously followed. Individuals and institutions, both Federal and contracted, must be held accountable for failure to follow established security measures. As it has begun to do so in response to the most recent Los Alamos incident, the Department should emphasize that the failure to properly protect classified information and materials will have meaningful consequences.

Finally, consistent with our 2006 recommendation, we continue to believe the Department should perform a risk-based evaluation of cyber security funding at Los Alamos. The objective of this evaluation would be to ensure that the resources are available for complete implementation of the revised cyber security policies and procedures.

For the past 5 years we have identified both cyber and physical security as pressing management challenges. For these reasons and because of the recent incidents, the Office of Inspector General continues to be concerned about the security across the Department of Energy complex. We have ongoing activities to examine information technology and system security, implementation to revise security measures, disposal of sensitive property, and issues related to protective force training.

In addition to our ongoing work, the full committee in January 2007 requested that the GAO examine the security of the Department's unclassified and classified information networks and its cyber security programs. My office coordinates closely with GAO on reviews of the Department, and we are hopeful that he assessment requested by the committee will provide recommendations leading to a strengthened agency-wide security posture. My office continues to conduct audit inspection investigative work that complements the reviews requested by the committee.

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

[The prepared statement of Mr. Friedman appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you, sir. Next we will hear from Mr. Anastasio for 5 minutes.

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

Mr. ANASTASIO. Good afternoon, Chairman Stupak, Ranking Member Whitfield, and other members of the committee. Thank you for the opportunity to update you on our progress.

As you know, I am Michael Anastasio, Director of the Los Alamos National Laboratory since June 2006 and president of the Los Alamos National Security, LLC.

I am pleased to report that we have continued to make significant progress on many fronts since I last addressed this subcommittee 11 weeks ago. Today, in keeping with the subject of this hearing, I will focus on security; and I want to reiterate what I said at the last hearing, that I personally take the issue of security at Los Alamos very, very seriously.

First, we have significantly reduced risks in both cyber and physical security, and this includes reducing and consolidating classified holdings, per the subcommittee's stated concerns. Second, we have taken actions to make policy clear and consistent and to change employee behaviors. And third, we are putting in place comprehensive corrective actions with a major focus on long-term sustainability.

Here are some examples of the specific actions my management team, my Board of Governors, and I myself personally are taking to reduce risk. Starting with cyber security, we now have positive control over all our classified computer ports using a combination of software, physical locks, and tamper-indicating devices. All of our classified systems have been inspected and found to be compliant, and we have reduced the number of stand-alone classified systems by 28 percent.

As for physical security improvements, we have made our vault escort requirements clearer and tougher, for example, requiring the search of all belongings carried by those escorted both in and out of the vaults. By December, we will have reduced our accountable classified removable electronic media, known as ACREM, by 50 percent. We have destroyed almost 1,500 classified parts and 500 boxes of classified documents that we inherited. We have eliminated 14 vault-type rooms, a reduction of 10 percent, with more to come.

In the area of policy and behaviors, we have uniformly trained our Information Systems Security Officers, our ISSOs, and are hiring senior ISSOs in all key organizations to provide consistency across the laboratory.

We are clarifying and simplifying security policy. In addition to mandatory training, we will promote the right behaviors through active employee participation. For example, we have directly involved employees and worker-led security teams at multiple levels in our line organizations.

On March 5, we launched and enhanced substance abuse program where every newly hired employee is tested for illegal drugs and every badge holder is now subject to random testing, regardless of his or her clearance level.

For long-term effectiveness and sustainability, we have begun constructing a super vault-type room, the first of its kind. This will allow us to consolidate and uniformly control classified information

managed by security professionals. At the same time, it will give authorized users efficient access to this information. I expect to complete construction of the first functional prototype this June. This project will initially allow us to close six additional vault-type rooms and reduce our ACREM libraries by one-third. By constructing additional super vault-type rooms, we will reduce the number of classified vaults to an absolute minimum consistent with our operational and mission requirements.

We have also been careful to embed validation and verification regimes into our corrective action plans in order to sustain all of these efforts and to prevent any backsliding. Moreover, everything we are doing is being closely scrutinized, not only by Congress but by my own Board of Governors, by the DOE, NNSA, and other oversight bodies. I welcome that continuing scrutiny. It validates that we are heading in the right direction and keeps our eye on the ball.

So in conclusion, Mr. Chairman, as I have testified previously on this issue, there are no silver bullets where security is concerned, but with these security enhancements and Board of Governors' support and oversight, we are aggressively moving Los Alamos in the right direction as we are in many other fronts vital to our success as a national security science laboratory.

Thank you again for the opportunity to testify, and I am happy to take your questions.

[The prepared statement of Mr. Anastasio appears at the conclusion of the hearing.]

Mr. STUPAK. Thank you both for being here, and we will start with questioning that will go for 10 minutes. I am glad to see Mr. Udall is still here. It is Friday, the votes are over for the week, everyone has taken off, but Mr. Udall has great interest in this. He remains with us. Thank you again, Tom.

Before we begin, Mr. Friedman, I indicated I was going to ask you the same question I put to the Secretary about your testimony that the Federal and contractor managers need to be more aggressive. In fact, you said that in your opening statement and the Department must develop a regimen in compliance. However, we seem to have this pilot program at Los Alamos which really would reduce Federal oversight increase, contractor self-assessment. Do you believe that reduced Federal oversight is the appropriate model at this time? If so or if no, why not?

Mr. FRIEDMAN. I do not, Mr. Stupak. We have been following this proposal for several years.

Mr. STUPAK. So you are familiar with this pilot project?

Mr. FRIEDMAN. Yes.

Mr. STUPAK. And it has been around for a number of years?

Mr. FRIEDMAN. Yes.

Mr. STUPAK. It is it site-specific to Los Alamos?

Mr. FRIEDMAN. Well, I am not the expert as to how they are ruling it out, but it seemed to me it may have initiated at Sandia and it has some relationship to the Kansas City plant; but certainly it is contemplated for Los Alamos as well.

Mr. STUPAK. Right, the document I held up, the memo, was from Linton F. Brooks, the Administrator, and former ambassador. It's the pilot of the new National Nuclear Security Administration,

oversight model for Los Alamos. This is the document you are speaking of?

Mr. FRIEDMAN. I assume it is.

Mr. STUPAK. While we are here, I will wait until Ed gets back, but I would like to move for admission in the record. It actually says in December 2002 we announced a new approach to oversight with the National Nuclear Security Administration. So this is the pilot program we have been speaking about?

Mr. FRIEDMAN. Yes, this memo is not dated and I am not sure when I did see it.

Mr. STUPAK. It is signed by Ambassador Brooks?

Mr. FRIEDMAN. It does appear to be, yes.

Mr. STUPAK. Why would a Secretary not know about a memo dealing with Los Alamos as to a pilot of the new National Nuclear Security Administration oversight model for Los Alamos?

Mr. FRIEDMAN. I certainly cannot testify on behalf of the Secretary on that. I really don't know.

Mr. STUPAK. Should the Secretary be made aware of it?

Mr. FRIEDMAN. The span of activities in the Department of Energy is enormous, and perhaps he was aware of it under some other name. I just can't speak for him.

Mr. STUPAK. OK. I also asked the Secretary about the cell phone in a vault. Do you have any knowledge of that in your overview about this employee had a cell phone in a vault?

Mr. FRIEDMAN. Mr. Stupak, as I recall your background, I think you have a law enforcement background.

Mr. STUPAK. Yes.

Mr. FRIEDMAN. And I am ill at ease answering your question. There is an ongoing FBI investigation with deep involvement of the Justice Department and the question of the individual's background, and what is in her investigative file is certainly part of that investigation. And I would not want to say anything inadvertently in response to your question that would compromise that. I am familiar with at least one incident, and there was an allegation of a second incident.

Mr. STUPAK. Of a cell phone in a vault?

Mr. FRIEDMAN. Right.

Mr. STUPAK. It is an unsecured cell phone in a secured vault?

Mr. FRIEDMAN. Essentially that is correct.

Mr. STUPAK. OK. And is this a——

Mr. FRIEDMAN. I should say I think it is a personal cell phone.

Mr. STUPAK. Right. Personal or departmental but it was an unsecured cell phone. And is this a breach or violation of security at Los Alamos?

Mr. FRIEDMAN. My understanding it most certainly is or was.

Mr. STUPAK. OK. And again, if the Secretary is briefed about an investigation, if there are these allegations, he certainly should be made aware of it. You see, my problem is the last time we testified here in January we had the breach about the employee's personal information being put out on the web inadvertently, and the Secretary didn't seem to know about that or DOE Order 470, we don't seem to know anything about that, we don't seem to know anything about the cell phone. It seems like not only is there structural

problems within Los Alamos and DOE but it seems like there is a communication problem, too.

Mr. FRIEDMAN. Well, I think that the people most directly responsible for operations of the laboratory and the Federal site were aware of the incidents as best I could determine, and certainly we were aware of them. So the fact that the Secretary was not aware of them given the, again, the scope of his activities, I am not sure it is all that surprising.

Mr. STUPAK. The fact that you're aware of it, someone in DOE should be made aware of it.

Mr. FRIEDMAN. Yes, absolutely.

Mr. STUPAK. What's the problem with this pilot program here? What are your concerns specifically? Does it lead to less Federal oversight and more self-assessment by the contractor?

Mr. FRIEDMAN. I am not the best person to testify on the program itself, but the essence of it is as you characterized it, reliance on self-assessment with a third-party review of the assessments, similar to commercial standards. I mean, that's basically what we're talking about.

We have for many years been concerned, we have expressed this in a number of forums, about the effectiveness of the Department's administration of its contracts. And it is our view that sort of stepping back, while it may be satisfying for the contractors because it means less reports, less intrusive reviews, less evaluations, is not the approach that we should take.

Mr. STUPAK. It is not the aggressive approach that you've been suggesting?

Mr. FRIEDMAN. No, it is not.

Mr. STUPAK. OK. The 550 security police officers went on strike at Pantex. I think Mr. Burgess mentioned it on the first span on his opening there, and there is a force of about 211 to replace them. Given your reduction in force size, and I understand some people have to work up to 84-hour workweeks, can you give an opinion whether the Nation's most valuable nuclear assets are being protected at a level that is sufficient to meet Department requirements?

Mr. FRIEDMAN. I don't know how many people and I accept your numbers, Mr. Chairman, and I don't quarrel with them. We issued a report I think last year at the Oak Ridge complex in which we were concerned about the amount of overtime, that it was excessive and it would lead to a degradation of the ability of the guard force. And I take it that the guards that have been sent to Pantex have been sent from other locations throughout the Department complex. So certainly to the extent that we have been concerned historically about overtime and the impact of the overtime on the ability of the guards to do their job, there is that concern.

Mr. STUPAK. Well, besides the drawing of personnel from other areas of the other sites to beef up Pantex while we have this security police that went on strike there, what would be the longer-term consequences to the Pantex site operations if this dispute goes on for a protracted period of time? I guess my concern is Pantex, where we assemble everything and disassemble, seems like it is one of the more sensitive sites. So if this goes on for a protracted

period of time, that is going to lessen our security I would think overall.

Mr. FRIEDMAN. Let me divert for just 1 second. I should tell you that in the interest of full disclosure that there are five or six points that have been expressed to us by the guards themselves and other individuals, and we are pursuing those aggressively. Now, we have an open inspections on those fundamental issues. And they do deal with core safety and security. I am not in the position to evaluate what the short-term, mid-term, or long-term impact of a strike would be. I think it is pretty clear that this is one of the most sensitive sites that the U.S. Government has in the continental United States, and it is a situation which needs to be resolved as soon as possible or there will be potential consequences.

Mr. STUPAK. Thank you. Mr. Anastasio, I was a little concerned when the Secretary testified, and I think you were in the room then, about the memo here to do the implementation of your cyber security I believe it was, that the booklet was given to your organization right around March 8, you have 90 days to comment on it, you send it back to the Department, and then he said it would be years to implement it. Why would it take years to implement the policy?

You get 90 days, why would it take years to implement it.

Mr. ANASTASIO. Well, it is a complicated set of requirements that takes——

Mr. STUPAK. It is complicated to digest and 90 days to——

Mr. ANASTASIO. Excuse me? I am sorry, I didn't hear it.

Mr. STUPAK. You have 90 days to digest it.

Mr. ANASTASIO. Ninety days to comment and then we will have to put in place a plan that will do the implementation over a specific period of time; and then of course, we will have lots of oversight and the effectiveness of carrying out that plan, both to put it in place and to make sure that we have an effective plan in place as we do that.

Mr. STUPAK. I mentioned and the Secretary objected to this, your new organization managing Los Alamos, is made up of UC people. What percentage? I said 60, he said it was not 60. What is it, do you know?

Mr. ANASTASIO. The management is an equal partnership of the two major partners of the UC and the Bechtel National.

Mr. STUPAK. So if it is equal, is it 50 percent then?

Mr. ANASTASIO. Yes, so as an example, the executive committee of the board has six members, three from the university and three from the industrial partners, so in that sense it is——

Mr. STUPAK. OK. What about the board makeup then?

Mr. ANASTASIO. There is the executive committee as I said and then there are an additional five members from outside any of the partner companies. Overall 11, but let us say the business decisions of the LLC are made by the Executive Committee. That is three and three.

Mr. STUPAK. OK. And that is 50 percent then basically?

Mr. ANASTASIO. Yes, sir.

Mr. STUPAK. OK. I guess my time has expired. Mr. Walden for questions?

Mr. WALDEN. Thank you, Mr. Chairman. I appreciate that. Director Anastasio, in your testimony you pointed to progress at the site by stating, and I quote, "we have destroyed 500 boxes of classified documents we inherited at Los Alamos." Sounds like a lot of documents. However, I am told when the committee staff asked about how many classified documents there are at Los Alamos, to try and put this in perspective, the lab's response was there is no requirement to maintain strict accountability of each classified document. We cannot tell you how many classified documents we have which leaves some of us wondering, do you know how many classified documents you have and there is no system in place to monitor those?

Mr. ANASTASIO. There is a set of specific kinds of classified documents that we are required to keep in an accountability system where we have a strict numbering system on every individual document, and we track those. But the general large collection of documents that we have, there is not a requirement to keep it in strict accountability system.

We do protect those documents in a very rigorous way.

Mr. WALDEN. I understand the need to do that. I guess I am just trying to put your comment in perspective because I don't know how big the boxes are.

Mr. ANASTASIO. Oh, I am sorry. So we have probably I would estimate, I don't have an exact count, but I would estimate that we have several million classified documents.

Mr. WALDEN. And so I guess the question is I have heard estimates of up to 30 million classified documents?

Mr. ANASTASIO. That sounds high to me, but again, I don't have an exact number.

Mr. WALDEN. When you say you have destroyed 500 boxes of classified documents, is that 1,000 documents or is that 10,000 documents?

Mr. ANASTASIO. There are, kind of——

Mr. WALDEN. Just sort of file folder box documents?

Mr. ANASTASIO. Yes, file folder boxes, yes, sir.

Mr. WALDEN. So it wouldn't be that many then?

Mr. ANASTASIO. Not in relation to the total number. All I was——

Mr. WALDEN. That is what I am trying to do is get it in perspective.

Mr. WALDEN. Yes, sir.

Mr. ANASTASIO. All I was trying to express is that we are actively in just the last 11 weeks off working down the large volume of both documents, parts, removable media, vault-type rooms and so forth. We have a concerted effort we have moved out on, and there is really concrete progress that we have made just the last 11 weeks.

Mr. WALDEN. And I appreciate that. I think that is a good thing. How many boxes would normally be destroyed in a given year? I assume this is like my business where you are always shredding things from the prior year, and you are kind of keeping the shelving available as you move forward another year.

Mr. ANASTASIO. Unfortunately, my impression at Los Alamos is they have not destroyed many things very often.

Mr. WALDEN. Classified as pack rats then?

Mr. ANASTASIO. So they keep labeling things and store them and to keep good records. Now we have good computer systems that we can scan and upload documents into a computer system that we can actually use the information more effectively that way because you can search it just like you would information on the Internet but in a classified network, in a classified computer, protected. Then that obviates the need for the document and we can start getting rid of documents. So there is a very active program and a very active desire on our employees, in fact, to move that way because it is easier to manage.

Mr. WALDEN. Sure. We obviously, and I have, made reference to the J.B. Weld project of security enhancement at the labs, and I have had our prop here to point out a simple solution. I suppose the more simple solution would have been to order computers that don't have USB ports to begin with, rather than glue these shut.

As you replace computers, which I assume the lab is doing, are they ordering computers with USB ports in them or are they ordering them without USB ports in them?

Mr. ANASTASIO. Most computers have a USB port as an example to plug the keyboard in. That is through USB port, and of course, you need a keyboard on the computer. In some cases some computer you actually want to get information off the computers and you need a mechanism to do that. But what we have done is we have put controls in place that, for instance, even if you have a keyboard with a USB port plugged in, you can put software in place as an example that makes sure that that port only recognizes the keyboard.

Mr. WALDEN. Right.

Mr. ANASTASIO. If you try to put a fun drive or the equivalent into it, the computer doesn't recognize what it is, it is incapable of reading that. When we move to this super vault-type rooms that I alluded to in my testimony, what we are looking at right now as part of this prototype is to have what I like to call an idiot savant computer, a computer that is very, very capable at displaying data but is very stupid at doing anything else. And so it doesn't have the operating system capability to recognize ports to do anything. So there is a keyboard, there is a mouse, and it can display 3-D very rapidly, high-resolution data, but it can's process the data. That is done on the server that is locked up in this vault, protected by people who are security professionals with a different approach to security when done in the past.

So that is the direction we are trying to move to really move away from being even concerned about whether you have a port or not, you are just going to disable it so that it can't function at all.

Mr. WALDEN. And clearly it is not really our job to micromanage the security of your labs, but it is our job to make sure somebody is doing that. And so I know we have all gotten to know each other all too well in the last few months and years. We couldn't spend this time on every agency, but I can't think of one that is more important to American security in many respects than the one that you are in charge of. And so I just still struggle at how these opportunities to lose data occur as we saw I think it was last fall with the woman who took the data home and was working out of her home and then got caught. And I guess I just still struggle, won-

dering how is it so hard to fix? I mean, you were at Lawrence Livermore before, right?

Mr. ANASTASIO. That is correct.

Mr. WALDEN. And you didn't see these kinds of breaches of security at Lawrence Livermore, did we? Did you?

Mr. ANASTASIO. Not of this nature, no.

Mr. WALDEN. So what is different here? I mean, you have been there a while now. What is going on? I mean, you got good people, I'm sure, at both labs, top-notch brains, scientists, but the security function just seems to be a problem.

Mr. ANASTASIO. Well, I think there is a variety of issues. I think having the right leadership team and the people who are focused on this, to bring a system-level approach to it, to have consistency and simplicity so the employees can understand, actually making systems so that employees can succeed, people are human. They are fallible. People make mistakes. So we need to put in place a system so that if there is a mistake that we contain any potential impact of the mistake. This is standard but kind of safety approached in human performance from the nuclear power industry, as an example. These are systems that so if you start to drift off, there is something to remind you, hey, you are starting to make a mistake, you need to stop. And that happens before there is any significant consequence.

So these are the kinds of systems we are trying to put in place to really make sure the employees can be a success, they are very committed to our national security, they are very conscious and conscientious about security in this sense. And so my job is to make sure that I give them all the tools they can have to be a success and at the same time hold them accountable for my expectations of them. And if they really intentionally violate the rules, then there are severe consequences for that.

Do you find many who intentionally violate the rules?

Mr. ANASTASIO. No, sir. Since June if I remember correctly, I think we terminated one employee for violating security rules. That is my memory, on the order of one or two.

So it does happen. We will take the action to terminate someone, but it is not very frequent at all.

Mr. WALDEN. Mr. Friedman, are you comfortable with what I am hearing here today from your independent perspective that things are going to turn around soon?

Mr. FRIEDMAN. Mr. Walden, I guess that is the question that I hope I wasn't asked.

Mr. WALDEN. Now I am doing my job.

Mr. FRIEDMAN. Einstein, I think, said that insanity is doing the same thing over and over and expecting a different result.

Mr. WALDEN. Expect a different result.

Mr. FRIEDMAN. As I testified in January, I am really hopeful that the new management team at Los Alamos and the Department's aggressiveness will result in a meaningful change in the way they view security and safety and the other operational issues that have been a problem there for so many years. Can I give you a level of guarantee? No. I hope it is the case, and it would serve everyone if that is the case.

Mr. WALDEN. So we need to plan on another hearing in a couple of months at which time you should be able to give us that certainty, correct?

Mr. FRIEDMAN. Only if you serve lunch for the next hearing.

Mr. WALDEN. Yes, well, hopefully it won't be a barbecue. With that, I yield back my time, Mr. Chairman.

Mr. STUPAK. I thank the gentleman from Oregon. The gentleman from Washington, Mr. Inslee for questions?

Mr. INSLEE. Thank you. Mr. Friedman, I have missed some of this but I wanted to ask you, what could you tell us specifically needs to be done that is not currently being done at the lab so that you can control classified and unclassified, sensitive information?

Mr. FRIEDMAN. Well, I think as the Secretary testified this morning that many of the corrective actions are a work in progress, and that has been historically one of the problems it seems to me that we get off to a good start, we have good ideas, we try to implement good fixes, but they lose steam, the momentum is lost. So one of the important things that has to be done is that all of the good things that have been proposed, discussed here today, and have been reduced to writing in various forms are, in fact, implemented and they flow down to the entire organization. Again, one of the historic problems we found is that the upper levels frequently got it but it didn't always make it down to the 10,000 or so other people who work at Los Alamos. So that is one.

Second, I think we need to ensure that we overcome the resistance to change. Change is difficult for all of us but we the question was posed previously about the difference between Los Alamos and Livermore as an example. We have found historically that there has been strong resistance to change at Los Alamos. As much as I admire the laboratory and the work that they do and the people that are there, there is that resistance. And that has to be overcome. We have to make sure that the attempt to reduce the footprint that Dr. Anastasio described today, that is, reduce the number of vaults, consolidate, actually takes place. We have been advocating that frankly for a long, long time, and our recommendations simply have never been accepted. So there are some common-sense sorts of things that I think need to be done and can be done, and certainly the secretary has committed to it, as has Dr. Anastasio. And with the right set of oversight principles, I think we can hopefully make progress.

Mr. INSLEE. I want to ask Dr. Anastasio, I have been told that the DOE failed to incorporate the current safeguards and security requirements contained in Order 470 in its contract with LANS when the contract was signed in December 2005. Is that accurate?

Mr. ANASTASIO. My understanding is that the orders that were included did not include the appropriate language that civil penalties could result per the new 10 C.F.R. 824 order. So I believe, and I am not the expert on this, but I believe they were in the contract but it wasn't done in the right way to make them subject to this new order. But my understand is that has now been fixed.

Mr. INSLEE. Well, has that been fixed? Are those new orders contractually binding on the contractor now?

Mr. ANASTASIO. My understanding is that is the case right now, yes, sir.

Mr. INSLEE. OK. Thank you.

Mr. STUPAK. Mr. Whitfield for questions?

Mr. WHITFIELD. Thank you. Mr. Friedman, they didn't give you lunch today, is that my understanding?

Mr. FRIEDMAN. It doesn't show but no I didn't.

Mr. WHITFIELD. When we talk about Los Alamos, we are always talking about two basic issues, one, the footprint is way too bug, and then second, the culture, what I refer to as culture. And people keep talking about this resistance to change, and Mr. Anastasio, you have been at Lawrence Livermore and now you are at Los Alamos. How do you characterize this resistance to change? Is that something that is real or is this just something we just talk about?

Mr. ANASTASIO. I think it is real. I think there is a resistance to change, and I think all organizations have resistance to change, all individuals do. The employees at Los Alamos have been through very tumultuous times over the last many years, and there has been a lot of things happened to them. I think there is a lot of anxiety in the workforce, and that is one of my goals, of course, to stabilize the morale and get us focused on the future. And part of that is change, and I think the laboratory has not been through as much change at Los Alamos as I experienced at Livermore, having to face during my career there. But the goal I set out with the laboratory, I said let us think about it as improvement. It is not change to make your life worse, let us go decide what laboratory we want to be that is going to achieve all these goals that are hard to deny, and let us go create that laboratory, the laboratory we want to have, the kind that will serve us in the 21st century. And I find that employees are responding very much to that. But we have to take them through change. Change is a process, we all know, and we are in the middle of that process. We are not done yet. But I feel the laboratory has been very responsive. People want that kind of leadership, they want to move forward, they don't like the fact that they get talked about in hearings like this, and they are very receptive to doing the things they need to do to go forward for the future.

Mr. WHITFIELD. What are the total number of employees, including independent contractors?

Mr. ANASTASIO. I don't have an exact number off the top of my head, but around 13,000.

Mr. WHITFIELD. Right. But the morale has been low just because of this constant barrage of bad publicity and security leaks?

Mr. ANASTASIO. The constant barrage, the change of contractors, the change of directors. Los Alamos is used to having a director for 10 years, 20 years at a time; and over the last 5 years, maybe we have had three or four different directors. I mean, there is just this kind of change that has gone on that they are not used to, and so we have to move the employees through that.

Mr. WHITFIELD. Of course, you are the one responsible for doing this. How do you feel yourself about the progress that you're making right now?

Mr. ANASTASIO. I think we have made some really good progress as I tried to outline in my testimony, some examples of very concrete things that we have accomplished. I would be anxious to be able to do it even faster than we are doing. That would be my de-

sire, so I am pushing the system. But on the other hand, it is very important that we don't do this the way some things have been done in the past as well where you do Band-Aids because I think Mr. Friedman's comment, can we sustain this? If it is just one Band-Aid here and the next thing comes, there is another Band-Aid there. You are just moving from issue to issue. We need to put in place a system that is sustainable, that puts us not to catch up with the threat that we have but gets in front of it so that we can respond to the future threats. Cyber security is so difficult because computer technology advances so rapidly, and as that advances, that generates different kinds of threats. So we have to put into place a system that is really sustainable for the long term that puts us out in front, as well as putting in place the risk reductions immediately to handle the problems that we have today in trying to catch up to that. We are also trying to build a system that will serve us well into the future.

Mr. WHITFIELD. Well, we wish you the very best in this, and I think everyone in the country is really tired of the issue and hope to get it resolved; and I wish you the very best and look forward to continue working with you. I yield back the balance of my time.

Mr. ANASTASIO. Thank you, and we know that we have a special responsibility for the country; and we are taking that very seriously.

Mr. STUPAK. Mr. Anastasio, I have got a few questions if I may. Mr. Friedman, could you give him that memo that you were looking at earlier? The second paragraph of this memo from Linton Brooks, subject, Pilot of the New National Nuclear Security Administration Oversight Model at Los Alamos. The second line says, the arrival of a new management team at Los Alamos is an opportunity to take that action. Therefore, you are directed to move immediately into a 2-year pilot of our new oversight model once you have concurred in the Los Alamos National Security, LLC (LANS) Contractor Assurance System. Now that is your group, right?

Mr. ANASTASIO. Yes, sir.

Mr. STUPAK. So this pilot would apply to your group coming in to Los Alamos?

Mr. ANASTASIO. Yes, sir.

Mr. STUPAK. OK. So you would be familiar with this memo?

Mr. ANASTASIO. I am familiar with this, and I would like to just clarify one thing about this pilot and I do know about it, of course, and we are off doing our part. This of course is a memo to the site manager to the Federal workforce, not to us. But one thing to be clear on, it was very clear to me and still is that this is something that does not apply to security, it is something that does not apply to nuclear safety and biohazard facilities. This is something that applies——

Mr. STUPAK. It deals with the overall management of this site.

Mr. ANASTASIO. It deals with overall management.

Mr. STUPAK. And look what it says.

Mr. ANASTASIO. The oversight model of security and of nuclear operations has not changed because of this pilot. This pilot is about other things like——

Mr. STUPAK. Mismanagement of this site. It is totally related, whether you are dealing with classified, unclassified, employees

using drugs, not using drugs, cell phones, not using cell phones. It is the whole thing. And it says right here, the arrival of a new management team. You alluded to it, Mr. Friedman alluded to it. You come into a new management team, you are all fired up here to do something but then 6 months we lose the enthusiasm, nothing filters down. So instead of having more Federal oversight we are having less Federal oversight with self-assessment by the new management team, the new management team which has financial incentives to do well in their assessment. It seems like the fox is guarding the hen house in a way.

Mr. ANASTASIO. Just to clarify again, sir, that there is two issues. There is the management system I use inside the laboratory and how we manage the laboratory and what tools we use to do that——

Mr. STUPAK. Right, and we are trying to get at how are you going to be different from the other teams.

Mr. ANASTASIO. That is our Contractor Assurance System that is outlined here. This is the management tool I use for all activities.

Mr. STUPAK. OK.

Mr. ANASTASIO. That management system is transparent to the Federal Government so that they can see my dashboard, how I am doing against metrics. There is a second issue which is how does the Government provide oversight. In this pilot, the Government will maintain the same level of oversight, if not enhance it as what is going on now in things like security and like nuclear safety. The pilot is to try to change the oversight model for things that aren't that. So there is a management system which is our Contractor Assurance System which is my system——

Mr. STUPAK. And the pilot provides less oversight from a Federal point of view, from a DOE point of view?

Mr. ANASTASIO. But not for security.

Mr. STUPAK. OK. Then let us look at our dashboard, the figure we have looked at today, these charts we have had up once or twice from opening that.

Mr. ANASTASIO. Yes, sir.

Mr. STUPAK. In 2006, DOE's Office of Health, Safety, and Security found failing or substandard security performance in 14 of the 17 key areas—that is the chart over there—including classified material protection and control, cyber security, and emergency management. The trend was negative compared to 2002. Mr. Podonsky, the head of that office, testified on January 30, our last hearing, that "Los Alamos received the lowest set of performance ratings for security and emergency management since 1999." As you are looking at your dashboard, what explains it? Why are we going downward in our performance, security, cyber security?

Mr. ANASTASIO. Just to recall that audit was done last fall, between October and December of last year. Of course, I am very aware of it and was very concerned by it. We have taken a number of specific actions to address those issues. I have outlined a few of the concrete results of that. The other thing I would say is that many audits and reviews have been done since Mr. Podonsky's review that you are referring to, and just over the last few weeks, Mr. Pike, the DOE CIO, was here——

Mr. STUPAK. Right.

Mr. ANASTASIO. Not here, was at the laboratory as well as the NNSA CIO; and in talking to those folks after the review, they believe that in fact we have made very significant progress, that we have improved relative to——

Mr. STUPAK. So what changed the colors on that chart? What changed the red to something other than red, the yellow to at least green, and maybe we can get a blue one on there some day. How do we do it?

Mr. ANASTASIO. Well, I think those are the steps that we have been taking that I have outlined for you today and that I believe that I have tried to demonstrate that we are very serious about this, that we are taking very specific actions, that they are very concrete. Some have resulted in very demonstrable improvement, that we are continuing to focus on making those improvements, and at that same time getting it in a way that is sustainable, that we don't have to be back here——

Mr. STUPAK. Look at your dashboard, look at your speedometer. You got another one of these reviews coming up I believe this fall.

Mr. ANASTASIO. Yes, sir.

Mr. STUPAK. How fast are we going to be going? What colors are we going to see on there?

Mr. ANASTASIO. Well, I want as many greens up there as I can get. That is my goal.

Mr. STUPAK. OK. On March 28 an employee discovered that 550 employee names and Social Security numbers were posted on the Web site of a former subcontractor and worked for the former company, Lujan Software Service, to remove this information. Do you have any idea how long that information about these employees were on the Web site?

Mr. ANASTASIO. We are still investigating that issue right now, Mr. Chairman, so I don't know for sure how long it has been there. We believe the data is from the 1998 period is how long it has actually been up on the Web site, we have been working with Mr. Lujan and his company to try to do some forensics on the Web site to see if we can understand——

Mr. STUPAK. Right. It didn't have a counter, so we don't' know how many hits it has had.

Mr. ANASTASIO. We are working that. We don't have an answer to that.

Mr. STUPAK. It is from 1998 personnel records and was just discovered in 2007, so it has been there maybe 9 years?

Mr. ANASTASIO. It is potentially that. On the other hand, the information was a name and a Social Security number.

Mr. STUPAK. Right.

Mr. ANASTASIO. That information was buried in several layers down inside that Web site of a relatively small company. So we are hopeful that there has been little opportunity to compromise it. The second thing that we have done, of course, my first concern in this whole incident was for the employees themselves and we have taken a number of actions to support the employees. And I could go through those, but my point was going to be that in fact we have informed all the employees who were affected. We have heard back from none of them that say that they had a concern that they think that their information might have been compromised.

Mr. STUPAK. From this side I tell you, it would be a violation of the contract or subcontract to have this information out there.

Mr. ANASTASIO. Certainly part of his subcontract was to protect the personal information.

Mr. STUPAK. Then what action or accountability has been taken for Lujan Software Services?

Mr. ANASTASIO. Well, certainly we have made sure that we took down that information off that Web site. The lawyers and working with the IG, we are doing the investigation to understand what the——

Mr. STUPAK. So no enforcement action then?

Mr. ANASTASIO. Have yet but we are still in the middle of the investigation.

Mr. STUPAK. OK. The Inspector General testimony calls for a risk-based evaluation of cyber security funding at Los Alamos to make sure that the resources are available for revised cyber security policies. Has your organization undertaken this evaluation? When will it be complete? And do you have an estimate of that potential cost?

Mr. ANASTASIO. Yes, every year of course we given input to the Department on our funding requirements to meet the goals that they set out for us. So we do that every year. In addition, we have been in discussion with the Department about extending this idea of super vault-type rooms and made some estimates of what that might cost to—if this works like we hope, which we will learn as we run this pilot. We have been discussing with them as well what it would take to propagate that through the site in the way we would like over several years.

Mr. STUPAK. Do you have any numbers or anything for us?

Mr. ANASTASIO. I think it is premature to tell you what the number is. I think we have made some very simple estimate. Let me just say many tens of millions of dollars.

Mr. STUPAK. OK.

Mr. ANASTASIO. I hope that is useful.

Mr. STUPAK. Well, I said earlier, it is not get out of jail free, it is not Monopoly, it is not paper money, it is taxpayers' money and the monopoly—let me ask you a little bit about that. You are at Sandia. Did you have the contract at Sandia, too? Did you manage that lab?

Mr. ANASTASIO. No, it does not.

Mr. STUPAK. Is this the only lab where for 63 years, basically the life of this lab, one entity has had responsibility there?

Mr. ANASTASIO. It is certainly the only one in 63 years because Los Alamos was the first lab, of course, of that nature. The Lawrence Berkley Lab also has been under the UC contract. It is not a national security site but it is a DOE laboratory. But then the PNL Lab up in Washington has been under the same contractor, and I think that is coming up for competition and I don't remember exactly when but in the near term. So there are other sites that have had one contractor for many decades but——

Mr. STUPAK. Well, if you have open contractor, we have Secretaries come and go and members come and go and there is really no incentive to make that change, to bring forth any kind of change it seems like if you are always getting the same contract and no

matter how many hearings we have and things like this. And your board is still 50 percent UC.

Mr. ANASTASIO. But as you said to me or the committee or subcommittee said to me earlier in a question, why didn't we see these problems at Livermore, and I spent most of my career at Livermore which was under UC contract, too. So I don't think these problems are fundamentally an issue of the contractor per se, I think it is about the local situation more than it is the fundamental issue of the contractor. That is my personal view. But I would also say that I am very personally motivated to make Los Alamos a success. This is certainly something that I believe is very important for the country, and I can certainly speak for all the employees there, that they are very concerned about their role in these turbulent times the country faces to fulfill their role, to help the country's security.

Mr. STUPAK. No one questions your commitment to the process, but as we have heard over and over again from many, many people sitting in those chairs, they are all enthused, they are all excited, it goes for a while, it fizzes out, and it never seems to get down to the other 13,000 employees. We have the guards striking at places, performance reviews seem to go from bad to worse, and believe me, we don't like being here anymore than you do and having to got through these hearings.

Any further questions for anyone? I ask that the memo be made a part of the record, that our discovery book that we all agreed upon earlier be made part of the record except for the Official Use ones we will not make a part of the official record. We won't put the OU documents in.

With that we will keep the record open for 30 days and for follow-up questions for Secretary Bodman. I am sorry he had to leave. I am sure we will catch him back at another time, hopefully not in the real near future. And with that, we will let you go, Mr. Friedman. Get lunch and thank you for your time and effort. The hearing is adjourned.

[Whereupon, at 1:10 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

## TESTIMONY OF HON. SAMUEL BODMAN

Chairman Stupak, Congressman Whitfield, and Members of the Subcommittee, I'm pleased to appear before you to discuss what I consider to be one of the most pressing management issues confronting the Department of Energy (DOE). Since coming to the Department, one of my top goals has been to institute a safer, more secure work environment across the DOE complex. And I have meant this to include physical safety and security as well as cyber security. I want to be absolutely clear here: the protection of sensitive information is essential to our ability to meet our mission as a Department.

This testimony is intended to describe the steps that we have taken to improve security within the Department of Energy following last year's incident at Los Alamos National Laboratory (LANL). In particular, I will discuss improvements that have occurred since Deputy Secretary Sell last testified before you in January of this year. I would preface this discussion with two over-arching points: first, we have made significant progress over the past few months, and I am confident that we are on the right track. But, we are not satisfied. We are staying on top of this issue, and we continue to look for ways to identify and correct any potential weaknesses.

And I hasten to add that the entire senior leadership team at DOE—including myself, Deputy Secretary Sell, and National Nuclear Security Administration (NNSA) Acting Administrator Tom D'Agostino—remain strongly committed to im-

proving security at the entire DOE complex and to keeping this Committee closely informed of our progress.

SENIOR MANAGEMENT CHANGES AND DOE OVERSIGHT ACTIONS

First, let me describe the senior management and oversight changes that we have made at the Department level. In January, I made the difficult decision to replace the Under Secretary for Nuclear Security, and Thomas D'Agostino was named as the Acting Under Secretary and NNSA Administrator. In addition, NNSA has reassigned the Los Alamos Site Office (LASO) Manager and has put one of its strongest managers, Daniel Glenn—formerly of the Pantex Site Office, in place as Acting Manager. We are making changes to the Los Alamos National Security, LLC (LANS) contract to mandate further improvements, and we have increased the planned fiscal year 2008 investment in cyber security significantly.

In addition, following the event at LANL this past October, I formed two teams consisting of the Department's three Under Secretaries, the Chief of Health, Safety, and Security, and the Chief Information Officer: a Personnel Security Task Force and a Cyber Security Review Team. I asked them to make specific recommendations based on the Department's Inspector General report on the LANL incident.

The Personnel Security Task Force submitted its report on February 28, 2007. It recommended improvement in several areas. I have accepted their recommendations and have directed implementation to begin immediately of the following:

- Enhanced mandatory training for those involved in the granting of security clearances,
- Strengthened Departmental policy on drug testing for those that hold security clearances,
- Enhanced quality assurance oversight to increase confidence in the suitability of those granted a security clearance; and
- Revised the personnel security organizational structure to increase the authority and ensure greater accountability for the Personnel Security Program.

I have also directed that all of the recommendations made by the Cyber Security Review Team that have not already been implemented, be implemented immediately. To that end, issuance of a revised cyber security policy [DOE Order 205.1A] was completed on December 4, 2006. And, the new National Security Manual was issued on March 8, 2007. The Cyber Security Task Force also recommended the following, which we are in the process of implementing:

- Mandatory separation of duties for key positions, such as Information System Security Officers and System Administrators,
- Improved training for all individuals with cyber security responsibilities; and
- Improved line management oversight of cyber security.

We are also taking steps to further strengthen the oversight by NNSA of LASO. The NNSA Acting Administrator has directed the NNSA Chief Information Officer to work very closely with Site Office management to ensure cyber security requirements are implemented by LANL. To ensure that these requirements are fully implemented, the Designated Approval Authority position for cyber security has been strengthened within the LASO management structure. This position will report directly to the Site Office Manager and is in the process of being filled. Working in concert with the Site Office and NNSA management additional cyber security personnel will be hired to bolster the cyber security staff and program within the Site Office.

Further, Acting Administrator D'Agostino has requested that DOE's Office of Health, Safety and Security conduct annual inspections at Los Alamos for the next three years. This month, both NNSA's Office of Defense Nuclear Security and CIO will inspect LANL for the cyber and physical security programs. The Site Office will conduct annual surveys—and regular observations—of the Lab's security programs.

We are also exercising the Department's new authorities under 10 CFR 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations. The DOE Office of Enforcement has completed its review of the LANL incident and last week the Department held an enforcement conference with the Lab's current management and operating contractor, LANS, and with the former contractor, the University of California. Similar to the process we use for Price-Anderson enforcement, both contractors now have the opportunity to respond before we make a decision regarding a Preliminary Notice of Violation.

Finally, I would just add that I continue to be in close contact with the senior leadership of the Laboratory and the LANS Board.

CORRECTIVE ACTIONS BY LANL MANAGEMENT & OPERATING CONTRACTOR LANS, LLC

Even while these Departmental reviews and changes have been underway, LANS has moved ahead with corrective actions. Following the incident, LANS immediately strengthened its escorting procedures, initiated mandatory entry and exit inspections of vault-type room visitors, and increased the number of exit inspections at other security boundaries ten-fold.

One of the issues identified as a contributing cause to this incident was the span of classified activities. LANS continues on schedule to move to a diskless environment, reducing the number of pieces of classified removable electronic media (CREM) and the number of classified paper documents. LANL recognizes their volume of classified holdings is unnecessarily large, conducted in too many security areas, involves too many people, and is spread out over too large of an area. As a result, LANS is aggressively reducing the number of locations where they hold and process classified matter. LANS will more closely scrutinize the continued need for existing security operations or the establishment of a new security area. This will enable them to better focus professional security resources to provide stronger management and oversight of classified operations.

To achieve this reduction, LANS has proposed, and NNSA has approved, a new consolidated vault-type room (VTR) concept to create classified matter storage and processing centers thatwill reduce the number of security areas and enhance the accountability and control of classified matter. The first ″Super″ VTR is planned to open on June 1, 2007.

The Weapons Engineering Division at LANL plans to close three VTRs immediately, three more by the end of April, and another five by the end of fiscal year 2007, a reduction of 50 percent. This division also plans to further reduce its CREM holdings by 90 percent, from 364 to a dozen or so pieces in the near term. Another division within LANL, the Weapons Physics Division, currently has six VTRs; it will close three by the end of fiscal year 2007. The classified materials in these VTRs will be archived, destroyed, or re-located as appropriate. These reductions are just examples of progress that will reduce security risk without reducing the productivity of our scientists and engineers.

While this incident occurred during the early stage of LANS' contract, I hold it accountable for the incident, and for rectifying the situation, just as I would at any DOE site managed by any contractor.

The LANS Board of Governors has also taken an active role in reviewing and validating the adequacy of LANL's corrective actions. The Board is closely monitoring the Laboratory's integrated corrective action plan which was developed to address the root causes of the incident identified during the incident inquiry. LANS has reassigned cyber security responsibilities to the Chief Security Officer who reports directly to the Laboratory Director. The Board has also made a significant effort to employ the collective power of the LANS member companies through the use of Assess, Improve, and Modernize, or AIM Teams from the member companies to conduct oversight assessments and make recommendations for improvement. The Board has taken aleadership role in numerous other ways as well, but most importantly, it has opened a clear line of communication with me and the Acting NNSA Administrator. I talk to the Chairman of the LANS Board of Governors, Gerald Parsky on a regular basis. In fact, we met with the Chairman and Vice Chairman of the Board of Governors in person two weeks ago.

CONCLUDING OBSERVATIONS

While we have made significant improvements and changes in personnel and cyber security programs, I believe that in order to guard against future incidents, we must continually improve the security culture across the DOE complex. And we will.

In closing, let me just say this: the men and women who work at LANL and all our National Laboratories are among the world's most talented scientists and engineers. Since their founding, these Laboratories have demonstrated again and again the tremendous power—and promise—of science to help our nation solve its greatest challenges. But such a system cannot tolerate any lapses in security—be they in the physical or cyber realm. Protecting critical information and maintaining a vibrant, collaborative scientific culture are not mutually exclusive goals. Quite the opposite is true. In this case, you absolutely cannot achieve one without the other. And, you continue to have my word that I will do everything in my power to support both objectives. The American people deserve no less.

This concludes my statement. I will be pleased to respond to your questions. Thank you.

---

## TESTIMONY OF MICHAEL R. ANASTASIO

Good morning Chairman Stupak, Ranking Member Whitfield, and Members of the Subcommittee. Thank you for the opportunity to update you on our progress.

I am Michael Anastasio, director of Los Alamos National Laboratory since June 2006, and president of Los Alamos National Security, LLC.

I am pleased to report that we have continued to make significant progress on many fronts since I last addressed this Subcommittee 11 weeks ago. Today, in keeping with the subject of this hearing, I will focus on security. As I expressed at the last hearing, I personally take the issue of security at Los Alamos very seriously. We are entrusted with some of the Nation's most important secrets and I view their safeguarding as one of my most significant responsibilities.

First, we have significantly cut our risks in both cyber and physical security. This includes reducing and consolidating our classified holdings, per the subcommittee's stated concern. Second, we are taking additional actions to make policy clear and consistent—and to change employee behavior. Third, we are putting in place comprehensive corrective actions with a major focus on long-term sustainability.

My management team, my Board of Governors, and I are taking a number of specific actions to reduce risk.

**Cyber security.** We now have positive control over both our classified computer ports, using a combination of software, physical locks, and tamper-indicating devices. All of our classified systems have been inspected and found to be compliant. We have reduced the number of stand-alone classified systems by 28 percent.

**Physical security.** We have made our vault escort requirements clearer and much tougher, requiring the search of all belongings carried by those escorted in and out of vaults. By December, we will have reduced our accountable classified removable electronic media (known as ACREM) by 50 percent. We have destroyed almost 1,500 classified parts and 500 boxes of classified documents that we inherited. We have eliminated 14 vault-type rooms, a reduction of 10 percent—with more to come.

**Policy and behaviors.** In the area of policy and behaviors, we have uniformly trained our Information Systems Security Officers (ISSOs) and are hiring senior ISSOs in all key organizations to provide consistency throughout the Laboratory.

We are making our cyber security policy clearer and simpler. In addition to mandatory training, we will promote the right behavior through active employee participation. For example, we will directly involve employees through worker-led security teams at multiple levels.

On March 5, we launched an enhanced substance abuse program. Every newly hired employee is tested for illegal drugs, and every badgeholder is now subject to random testing, regardless of his or her clearance level.

**New type of vault-type room.** For long-term effectiveness and sustainability, we have begun constructing a super vault-type room, the first of its kind. This will allow us to consolidate and control classified information uniformly. At the same time, it will give authorized users efficient access.

I expect to complete construction of the first functional prototype by June. This project will initially allow us to close at least six more vault-type rooms and reduce our ACREM libraries by nearly one-third.

By constructing additional super vault-type rooms, we will reduce the number of classified vaults to an absolute minimum, consistent with our operational requirements.

**Validation, verification & oversight.** We have been careful to embed validation and verification into our corrective action plans to sustain all these efforts and to prevent backsliding. Moreover, everything we're doing is being closely scrutinized only by Congress but by my own Board of Governors and by DOE, NNSA, and other oversight bodies. I welcome that continuing scrutiny. It validates that we're heading in the right direction—and keeps our eye on the ball.

As I testified previously on this issue, there are no "silver bullets" where security is concerned. But, with these security enhancements, and Board of Governors support and oversight, we are aggressively moving Los Alamos in the right direction, as we are on many other fronts vital to the Lab's mission.

Thank you again for the opportunity to testify. I would be pleased to answer any questions you may have.

---

## STATEMENT OF GREGORY H. FRIEDMAN

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on the concerns expressed in your April 5 letter regarding operations at the Los Alamos National Laboratory.

### BACKGROUND

In January of this year, I testified before this subcommittee on the special inquiry conducted by my office regarding the diversion of classified data from the Los Alamos National Laboratory. Specifically, at the request of the Secretary of Energy, we examined the efforts of the Department and its contractors to protect classified information and the steps that were taken to ensure that only authorized individuals had access to such information. Our report on this matter was issued on November 27, 2006.

### OFFICE OF INSPECTOR GENERAL REVIEW

The Office of Inspector General (OIG) found that the security environment at Los Alamos was inadequate, despite the expenditure of millions of dollars by the National Nuclear Security Administration to upgrade various components of the Laboratory's security apparatus.

In particular, related to the cyber security control structure, we found that:

- Certain computer ports, which could have been used to inappropriately migrate information from classified systems to unclassified devices and computers, had not been disabled;
- Classified computer racks were not locked;
- Certain individuals were inappropriately granted access to classified computers and equipment to which they were not entitled;
- Computers and peripherals that could have been used to compromise network security were introduced into a classified computing environment without approval; and,
- Critical security functions had not been adequately separated, essentially permitting system administrators to supervise themselves and override controls.

In many cases, Laboratory management and staff had not: developed policies necessary to protect classified information, enforced existing safeguards, or provided the attention or emphasis necessary to ensure protective measures were adequate. Some of the security policies were conflicting or applied inconsistently. We also found that Laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and physical inspections. In short, our findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

The OIG also reviewed certain aspects of the security clearance process in place for Laboratory employees. We identified particular weaknesses associated with this program which were discussed in a closed session of this subcommittee in January of this year.

### DEPARTMENTAL RESPONSE

After this incident was discovered, Department and Laboratory management officials launched several efforts to identify and correct control deficiencies that contributed to an environment in which classified information could be removed without authorization. In particular, the Deputy Secretary directed an immediate review of policies and practices related to computer ports at each of the Department's facilities. Further, the Secretary established two high-level Task Forces to address our findings. The reports of the Secretary's Task Forces and a list of the proposed corrective actions were provided to my office last week.

The report from the Department's Committee to Review the Cyber Security-related Recommendations indicated concurrence with the OIG's report and specified that the Department had initiated corrective actions that involved revising policy, securing unneeded ports, limiting access and privileges, and maintaining separation of duties. The report also indicated that controls over security planning and accreditation and physical inspections were to be strengthened and that corrective actions would be tracked to resolution.

The Personnel Security Program Review Task Force analyzed the OIG report and agreed that there were personnel security program weaknesses. The Task Force addressed the security clearance issues raised in our November 2006 report. Specifically, it identified and developed recommendations for improving Department-wide training, policy, quality assurance and oversight, and organizational structure. Addi-

tional details are contained in the Task Force's report, which has been marked by the Department as "Official Use Only."

Many of the corrective actions outlined by the two Task Forces are in progress. However, implementation and execution are key. If properly carried out, the corrective actions should improve classified operations at Los Alamos and could help prevent similar incidents at Departmental facilities around the complex.

### Issues Requiring Continuing Attention

As I have testified on several occasions, the Department must do a better job addressing the recurring challenges it faces. Specifically:

1. With regard to the current matter, the Department must ensure that all actions and recommendations outlined in the Task Force Reports are formalized into policy and adopted as practice throughout the Department. As part of that effort, these policies should be incorporated into all facility contracts.
2. To achieve the recommended reforms, the Department must establish firm schedules with specific implementation timelines and performance metrics.
3. Both Federal and contractor officials need to manage more aggressively. As part of that process, the Department needs to ensure that its Federal contract management function is adequately staffed and that the skill mix is appropriate. In addition, Department and Laboratory officials must develop a more comprehensive regimen of compliance testing and follow-up to ensure that security policies and procedures are rigorously followed.
4. Individuals and institutions, both Federal and contractor, must be held accountable for failure to follow established security measures. As it has begun to do in its response to the recent Los Alamos incident, the Department should emphasize that the failure to properly protect classified information and materials will have meaningful consequences.

Finally, consistent with our November 2006 recommendation, we continue to believe that the Department should perform a risk-based evaluation of cyber security funding at Los Alamos. The objective of this evaluation would be to ensure that the resources are available for complete implementation of the revised cyber security policies and procedures.

### Ongoing Inspector General Efforts

For the past 5 years, we have identified both cyber and physical security as pressing management challenges. For these reasons, and because of the recent incidents, the Office of Inspector General continues to be concerned about security across the complex. We have ongoing activities to examine information technology and systems security; implementation of revised security measures; disposal of sensitive property; and, issues related to protective force training.

In addition to our on-going work, the full Committee, in January 2007, requested that the Government Accountability Office (GAO) examine the security of the Department's unclassified and classified information networks and its cyber security programs. My office coordinates closely with GAO on reviews of the Department, and we believe that the assessment requested by the Committee will lead to a strengthened agency-wide security posture. My office will continue to conduct audit, inspection, and investigative work that will complement the review requested by the Committee.

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