AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

RESULTS OF SECURITY INSPECTIONS AT THE DEPARTMENT OF ENERGY'S LAWRENCE LIVERMORE NATIONAL LABORATORY

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JULY 20, 1999

Serial No. 106–146

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
58–496CC WASHINGTON : 2000

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

FRED UPTON, Michigan, *Chairman*

JOE BARTON, Texas
CHRISTOPHER COX, California
RICHARD BURR, North Carolina
Vice Chairman
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
ROY BLUNT, Missouri
ED BRYANT, Tennessee
TOM BLILEY, Virginia,
(Ex Officio)

RON KLINK, Pennsylvania
HENRY A. WAXMAN, California
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

Page

Testimony of:

Podonsky, Glenn S., Deputy Assistant Secretary for Oversight, Office of Environment, Safety and Health, Department of Energy 7

Tarter, C. Bruce, Director, Lawrence Livermore National Laboratory; accompanied by: Martin Domagala, Richard Mortensen, Jim Hirahara, Dennis Fisher, Don Wentz, Bill Hensley, John Jones, and Barbara Stone 11

Turner, James, Manager, Oakland Operations Office, Department of Energy 19

Weigand, Gil, Deputy Assistant Secretary, Strategic Computing and Simulation, Department of Energy 17

RESULTS OF SECURITY INSPECTIONS AT THE DEPARTMENT OF ENERGY'S LAWRENCE LIVERMORE NATIONAL LABORATORY

TUESDAY, JULY 20, 1999

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

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Burr, Bilbray, Ganske, Blunt, Bryant, Klink, Stupak, Green, McCarthy, Strickland, and DeGette.

Also present: Representatives Norwood and Shimkus.

Staff present: Tom DiLenge, majority counsel; and Reid Stuntz, minority staff director and chief counsel.

Mr. UPTON. Good morning, everyone. The subcommittee will come to order.

The subcommittee is meeting this morning to hold a hearing on the results of recent security inspections at the DOE's Lawrence Livermore lab. After members and witnesses have been recognized for opening statements, the Chair will make a motion to hold the remainder of the hearing in executive session. The Chair will recognize himself for an opening statement.

This hearing is a continuation of a classified briefing held for members 3 weeks ago on the results of a recent DOE inspection of security at Lawrence Livermore. While that briefing certainly was illuminating, the ability of members and staff to question the witnesses, many of whom are here again today, was limited by the Department's decision to withhold the inspection report and related documents from the committee prior to that briefing.

Now that we do have the necessary materials and have had a chance to review the inspection report in detail, we have called today's hearing to dig deeper into some of the issues raised by this recent inspection. While much of what we discuss today will be classified and thus discussed behind closed doors, some of what we have learned so far is unclassified and can be and should be discussed publicly. In particular, those issues that bear on the seeming inability of the lab and Department to conduct effective security management and oversight, to provide accurate information about the state of security to policymakers in the Department, the White House and certainly in the Congress, and to take prompt

and effective corrective actions with respect to identified vulnerabilities.

For example, there are numerous references in the recent inspection report to past findings of a similar serious and recurring nature, findings that went uncorrected for years. In other cases, the lab and Department field offices failed during their own security reviews to identify serious issues found by the recent independent inspection team and apparently did not even evaluate some significant areas of potential security concern.

In still other cases, the lab and field office security assessments did reveal vulnerabilities similar to those identified by the outside inspectors, but either corrective action was not taken or the program officials determined that the risk was somehow acceptable; that is, until the independent inspectors recently put this unwanted spotlight on these issues. Despite the recurrence of unresolved deficiencies year after year, we have found that Livermore has never been financially penalized for these significant security problems by the Department in its annual performance evaluations, at least not in recent memory.

But even if Livermore had been given unsatisfactory security ratings by its Department managers, security measures impact only a very small portion of the financial performance fees that the lab can receive under the current contract. I believe that without a closer link between security performance and financial performance, lasting change at Livermore and elsewhere in the DOE complex will continue to prove elusive.

Finally, we have also learned from this recent Livermore inspection that we cannot always believe what we hear about the status of security reforms at the Department. In particular, the lab directors and Secretary Richardson announced with much fanfare back in March a 9-point plan to undertake ambitious computer security upgrades on an even more ambitious timetable, reaching significant milestones within 30 days. And we were told in mid-April that those milestones were reached or would be reached within those 30 days, permitting these computer systems to be brought back on line with enhanced security.

Yet now we find that not only did Livermore fail to reach some important milestones as claimed, but that the lab thought it didn't really need to do what it had promised to do. And we found out as well that some of what the lab directors and Secretary Richardson promised would be done simply is not technologically feasible at this time and certainly not within the 30 days, which causes us all to worry that either they do not know what they are talking about, or they are more interested in the sound of the message than the reality of computer security.

I hope to explore these and related topics in detail after we move into closed session. But I want to let the American people know that this committee will continue to press the Department and its labs, including Livermore, to make the necessary changes to improve their security. And we will continue to dig behind the rhetoric to unmask the reality so that policymakers in both the executive and legislative branches have accurate information upon which to make reasoned policy judgments in this area.

I thank our witnesses for appearing before this committee today, and I will recognize the ranking member, Mr. Klink.

[The prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON, CHAIRMAN, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

Today's hearing is the continuation of a classified briefing held for Members three weeks ago on the results of a recent internal Department of Energy inspection of security at Lawrence Livermore National Laboratory. While that briefing certainly was illuminating, the ability of Members and staff to question the witnesses—many of whom are here again today—was limited by the Department's decision to withhold the inspection report and related documents from the Committee prior to that briefing. Now that we finally have received the necessary materials and have had a chance to review the inspection report in detail, we have called today's hearing to dig deeper into some of the issues raised by this recent inspection.

While much of what we discuss today will be classified and thus discussed behind closed doors, some of what we have learned so far is unclassified and can and should be discussed publicly—in particular, those issues that bear on the seeming inability of the lab and the Department to conduct effective security management and oversight, to provide accurate information about the state of security to policy makers in the Department, the White House, and in Congress, and to take prompt and effective correction actions with respect to identified vulnerabilities.

For example, there are numerous references in the recent inspection report to past findings of a similar, serious, and recurring nature—findings that went uncorrected for years. In other cases, the lab and Department field offices failed, during their own security reviews, to identify serious issues found by the recent independent inspection team, and apparently did not even evaluate some significant areas of potential security concern. In still other cases, the lab and field office security assessments did reveal vulnerabilities similar to those identified by the outside inspectors, but either corrective action was not taken or the program officials determined that the risk was somehow acceptable—that is, until the independent inspectors recently put this unwanted spotlight on these issues.

And, despite the recurrence of unresolved deficiencies year after year, we've learned that Livermore has never been financially penalized for these significant security problems by the Department in its annual contract performance evaluations—at least not in recent memory. But even if Livermore had been given unsatisfactory security ratings by its Department managers, security measures impact only a very small portion of the financial performance fees that the lab can receive under the current contract. I believe that, without a closer link between security performance and financial performance, lasting change at Livermore and elsewhere in the D-O-E complex will continue to prove elusive.

Finally, we've also learned from this recent Livermore inspection that we can't always believe what we hear about the status of security reforms at the Department. In particular, the lab directors and Secretary Richardson announced with much fanfare back in March a Nine Point Plan to undertake ambitious computer security upgrades on an even more ambitious timetable—reaching significant milestones within only 30 days. And we were told in mid-April that those milestones had in fact been reached or would be reached within those 30 days, permitting these computer systems to be brought back on-line with enhanced security.

Yet now we find out that not only did Livermore fail to reach some important milestones as claimed, but that the lab thought it didn't really need to do exactly what it had promised to do. And we find out, as well, that some of what the lab directors and Secretary Richardson promised would be done simply is not technologically feasible at this time or certainly not doable within 30 days—which causes me to worry that either they don't know what they are talking about, or they are more interested in the sound of the message than the reality of computer security.

I hope to explore these and related topics in detail, after we move into the closed session. But I want to let the American people know that this Committee will continue to press the Department and its labs, including Livermore, to make the necessary changes to improve their security. And we will continue to dig behind the rhetoric to unmask the reality, so that policy makers in both the executive and legislative branches have accurate information upon which to make reasoned policy judgments in this area.

I thank our witnesses for appearing before this Subcommittee today, and I will now recognize Ranking Member Klink, for an opening statement.

Mr. KLINK. Thank you, Mr. Chairman for holding this follow-up hearing. This committee was responsible for the establishment of the Office of Security Evaluation back in the late 1980's because of previous security crises at the Nation's weapons facility. Yet the Congress and the country has been rocked again by allegations that year of espionage and poor security of all types at the Nation's weapons laboratories. Both the Rudman report and internal reports from the Department of Energy have made it clear that security directives, even when issued by the President of the United States, were ignored and even flaunted by the laboratories and their scientists.

Senator Rudman spoke eloquently of the arrogant culture of the laboratories but, inexplicably, he didn't think that the contractors who run the facilities were responsible for security, although their contracts specifically do give them those jobs. All we have to do is look at Dr. Tarter's testimony today to find out who is in charge. Dr. Tarter magnanimously states that he is committed to DOE, that he will fund and implement the Secretary's 9-point information security action plan. Until reading his testimony, I didn't know Dr. Tarter had that choice.

One of the key questions I hope that we can answer today, and I want to ask him, is whether Lawrence Livermore's contract gives the University of California the responsibility and the budget for providing security for the Nation's weapons secrets, and if he has ever been hindered by the Department from carrying out those responsibilities. Then I want to ask if he considers that this is an optional responsibility, depending on whether or not he would like to carry it out.

Surprisingly, the response in Congress to these new allegations has been to propose legislation to give the laboratories, the field offices that directly supervise them, and the Defense Programs operation more independence and lack of oversight than ever before. The Assistant Secretary for Defense Programs, who was finally asked to resign a few weeks ago, last week came before another House committee and said these problems were everyone's fault, but mostly they were not his. He was praised for his fine work. This is the same person who, according to testimony in the Senate by Notra Trulock earlier this year, stopped Mr. Trulock in 1997 from briefing former Secretary Pena about alleged spying at Los Alamos because it might have a negative effect on his budget request.

Nothing we have heard in our recent hearings gives any indication that these changes will have the desired long-term effect in security, safety, or in any other areas. Last week in the committee's hearing on the reorganization of the Department being proposed by various congressional committees, a variety of experts stated that these reorganizations would very possibly make the accountability situation worse than it is now. This can only have a negative effect on security efforts.

Two weeks before that, we held a hearing on radiation safety enforcement security at DOE weapons facilities, at which Lawrence Livermore Laboratory was prominently featured because of the assessment of the largest fine in history of the Department for safety violations. And, again, there was great frustration expressed by the

Department's enforcement staff because of the recalcitrant attitude of the laboratory and the failure of the field offices to force change.

The historically poor state of security at Lawrence Livermore's laboratory is more than evident from the lab director's testimony today of all the steps he is now taking to improve security. I must ask why these actions were not taken years ago. I look forward to obtaining a clear statement from Lawrence Livermore and the University of California of their responsibility for maintaining adequate security. Then perhaps the next time this happens, perhaps the Congress will not fool itself about where the blame should lie.

With that, Mr. Chairman, I yield back my time.

Mr. UPTON. Are there other members seeking to give an opening statement?

Mr. BURR. Mr. Chairman, just a brief one. I thank the chairman and I thank our witnesses for returning and for the addition of other ones. Let me suggest to you today that as we have looked at this, three things have popped up: culture, contractors and complacency, and I think those are the three areas that we need to deal with.

Culture, something that was not a factor over the last 12 months but possibly 12 or 20 years, the culture that has to be changed, and that in fact the inspectors have recognized and highlighted as one of the challenges that they have.

Contractors. From a standpoint that these in many cases are projects that have never been bid, we have to look at the relationship of the contract. We have to look at certain areas of the contract. One very glaring thing in your public statement, Mr. Tarter, is that you refer to the marginal rating in materials and control and accountability as in the Annual Report to the President. Yet the report to the President under materials control and accountability is unsatisfactory. Marginal and unsatisfactory are completely different, by definition, but I think this gets at the heart of the cultural and the complacency problem, that we read them as in fact the same. Complacency not only by contractors, but DOE, about a sense of urgency of addressing things that deal with national security, deal with security of any corporation about secrets or about sensitive material that they have.

I am hopeful that as we move through this, Mr. Chairman, that in a bipartisan way we can work with inspectors to make sure that we have an accurate way to gauge in the future not only our progress but our success at maintaining the safeguards and securities that are needed.

I thank the chairman for the time and I yield back.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman. I will be brief. Mr. Chairman, we have had a number of hearings on this whole situation, and I think back to the April 20 hearing in which we talked about the real fundamental problem is the lack of accountability; that when things happen we, the U.S. Government, are not holding people accountable. And I think that if we would do that, then these things would not recur with such frequency.

Let me go back to what we have learned. We have had these concerns brought up in 1976, 1982, 1988, 1992, 1997, and now 1998

and 1999. And we always get assurances things will be different, but they never are. They never are.

From the chairman's comments to Ranking Member Klink, to everybody here, they are frustrated and really not quite sure what we should do. So I think we should go back to our fundamental problem here, which is lack of responsibility and accountability.

So why we ever approved another 5-year extension for Livermore Lab is beyond me. I think we should start with accountability and responsibility and pull that contract today. Maybe then—maybe then people will understand we are serious about this. I am not trying to pile on anyone, but I am just as frustrated as anybody up here, and if we are really going to have accountability and responsibility, then let us begin by pulling that contract.

I yield back my time, Mr. Chairman.

Mr. UPTON. Other members? Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman. I just want to follow up on my colleague from Michigan's point. I believe that the only way you can change the corporate culture is you remove the people who are established in the culture of whatever, the corporation, and we just don't do that. And some are the rules that we have put in place protecting employees or contractors.

I would like to see swift change in that and I agree with my colleague from Michigan that we ought to—this is something we ought to micromanage for a while through yearly contracts, and I am willing to be involved in that. We have had enough, and I think the displeasure of Congress is going to be felt. I yield back the balance of my time.

Mr. UPTON. Other members?

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Thank you, Mr. Chairman. Today's hearing is the continuation of what I promised back in March. At that time, I promised that, in light of the breaking reports about lax security at our nuclear weapon labs, this Committee would take a long, hard look at security at each of the major Department of Energy nuclear facilities, whose general management falls within this Committee's primary jurisdiction.

But well before this recent security scandal, I directed Committee staff to work with the General Accounting Office to re-evaluate the status of security at these facilities. I did so because of the Department's poor history in implementing lasting reforms—the last wave of which occurred in the early 1990s under then-Secretary Watkins. That G-A-0 review is still underway, and today's hearing will complement that work by providing very timely information about one particular and troublesome lab—Lawrence Livermore National Laboratory in California.

Let me state at the outset that Livermore is not being singled out by this Committee for criticism. Nor do I believe it is the worst offender. But Livermore was the first of the major labs to receive an internal security inspection following the Department's claims of major security reforms. Despite all of the high-profile attention that this topic has received at Livermore and across the D-O-E complex since earlier this year, Livermore simply did not hold up well under this latest scrutiny. While we cannot discuss the specifics of the report's findings in this open session, I can say that some of them are simply stunning—and have left me scratching my head, wondering how on earth things like this could have been happening for so long at a nuclear weapons lab without someone standing up and saying "this must stop."

Well, let me say that this, indeed, must stop. It is clear to me that, without aggressive and sustained internal and external oversight, Livermore will never fully correct these deficiencies, and I hope that this Committee's efforts to shine a spotlight on Livermore's troubles will assist those within the lab and the Department who truly want to achieve reform rather than just talk about it.

I understand that the Department's internal inspection team is currently reviewing Sandia National Laboratory and plans to inspect Los Alamos in the near future as well. I expect that we will hold similar hearings on the findings of those inspections, too. I hope that the Committee will not have to be prevented from gaining timely information about those inspections as it was with respect to the Livermore report. It troubles me that the Department forced excessive delays and my issuance of subpoenas to secure important materials for today's hearing.

This Committee has the absolute right to gain real-time and candid information about security at the Department's facilities. I am not interested in DOE whitewashing, defensive posturing, or the Administration's "all is now well" spin. And I intend to continue to take whatever steps are necessary to secure security information in a timely fashion. If the Secretary needs to rearrange his schedule to keep one step ahead of this Committee's work, that's fine with me—I don't know what other issue could be more important to him right now anyway. But I certainly won't let the Department continue to delay our review of this matter, which is of pressing concern to our Nation's security and to the American public.

Thank you, Mr. Chairman, for your continuing focus on this matter.

Mr. UPTON. Okay. If not, if there are no further opening statements, the Chair will recognize our witnesses: Dr. Gil Weigand, Deputy Assistant Secretary for Strategic Computing and Simulation at the Department of Energy; Mr. Glenn Podonsky, Deputy Assistant Secretary for Oversight, Office of Environment, Safety and Health at Department of Energy; Dr. James Turner, Manager of the Oakland Operations Office at the Department of Energy; and Dr. Bruce Tarter, Director of Lawrence Livermore National Lab.

I think all of you are aware that this subcommittee is an investigative subcommittee and, as such, we have always had the long-term practice of taking testimony under oath. Do any of you have objection to doing that?

We also advise you that each of you, under the Rules of the House, you are entitled to be advised by counsel. Do any of you have desire to be advised by counsel?

If not, in that case if you would stand and raise your right hand, and also, I guess, include the folks that may be testifying with you later on.

[Witnesses sworn.]

Mr. UPTON. You are now under oath and you are now allowed to give, hopefully, a 5-minute summary of your written statement and we will start with Mr. Podonsky. Welcome back.

TESTIMONY OF GLENN S. PODONSKY, DEPUTY ASSISTANT SECRETARY FOR OVERSIGHT, OFFICE OF ENVIRONMENT, SAFETY AND HEALTH, DEPARTMENT OF ENERGY; C. BRUCE TARTER, DIRECTOR, LAWRENCE LIVERMORE NATIONAL LABORATORY; ACCOMPANIED BY: MARTIN DOMAGALA, RICHARD MORTENSEN, JIM HIRAHARA, DENNIS FISHER, DON WENTZ, BILL HENSLEY, JOHN JONES, AND BARBARA STONE; GIL WEIGAND, DEPUTY ASSISTANT SECRETARY, STRATEGIC COMPUTING AND SIMULATION, DEPARTMENT OF ENERGY; AND JAMES TURNER, MANAGER, OAKLAND OPERATIONS OFFICE, DEPARTMENT OF ENERGY

Mr. PODONSKY. Thank you, Mr. Chairman. I appreciate the opportunity to again appear before the committee to discuss the Office of Independent Oversight and Inspection of the Lawrence Livermore National Laboratory. Just for clarification, I am now the director of the newly created Office of Independent Oversight and Performance.

As you know, we provided a classified briefing to members of this committee on July 1 on the results of our May 1999 inspection of safeguards and security programs at the Lawrence Livermore National Laboratory. At the briefing, we also provided copies of the classified inspection report.

At this time, I would also like to introduce Ms. Barbara Stone who is sitting behind me, who is the Director of the Office of Security Evaluations. Ms. Stone was unable to appear at the July 1 briefing as she was away on a much needed vacation. At that briefing we had Mr. John Hyndman, who is now engaged in the inspection of Sandia National Laboratory where Ms. Stone and I will be proceeding immediately following this hearing.

For the benefit of those who were unable to attend the July 1 briefing, I would like to provide some background on who we are. My office is responsible for providing the Secretary an independent, impartial view of the effectiveness and safeguards of security, cybersecurity and emergency management policies and programs throughout the Department of Energy. The Office of Security Evaluations which performed the inspection at Lawrence Livermore National Laboratory is one of the three offices that report to me.

As you may recall, the Office of Security Evaluations was originally established in 1984 to provide the Energy Department an independent assessment on the effectiveness of safeguards and security policies and programs throughout the Department. Congressman Dingell and Congressman Bliley were instrumental in the formation of that office.

As part of Secretary Richardson's recent effort to strengthen independent oversight of safeguards and security, the Office of Independent Oversight and Performance has now been elevated to report directly to him.

Now, I would like to take a minute to provide an unclassified summary of the May Livermore inspection. Our overall conclusion was that improvements were being made at Livermore but significant weaknesses remained to be addressed. For example, we saw improvements in the intrusion detection systems and significant progress to improve classified information on computer systems. However, we identified weaknesses that warrant continued attention in a number of areas. One of the weaknesses involved inadequate vulnerability assessments of the Superblock which is the area at Livermore where special nuclear material is used and stored. We also noted weaknesses in some aspects of Livermore's ability to accurately measure some types of nuclear materials. Other weaknesses were evident in Livermore's programs for protecting classified and sensitive information.

We identified weaknesses in their methods for storage of classified parts and some of the control of access areas containing classified matter. We were also concerned about foreign nationals being able to access Livermore unclassified computers through dial-up access. We noted that some aspects of the 9-point security plan for cybersecurity, which is a plan for improving classified information, required some work. Let me emphasize that these weaknesses warrant significant attention and require prompt action; however, as I told this committee during the briefing on July 1, we believe that the responsible line managers which are here today from the Office

of Defense Programs, the Oakland Operations Office, and Livermore National Laboratory, are taking the inspection report seriously now.

Although the formal inspection ended in May, the Office of Independent Oversight has continued to follow up on the progress to address identified deficiencies. We have been in frequent contact with the responsible DOE and Livermore managers since the inspection ended. Our follow-up efforts indicated that corrective actions are underway. For example, at the time of our July 1 briefing to this committee and as part of our follow-up, my office sent our inspectors back to Livermore to review progress at Superblock in the areas of modeling and testing, which is needed to verify the effectiveness of the protective strategy and response plan at Livermore.

Since the May 1999 inspection, Livermore has developed and is implementing a program of testing and modeling that is appropriate for verifying the effectiveness of protective force response. Livermore has also placed additional protective force personnel in the Superblock to improve response capability under the new protective strategy as defined. The Office of Oversight will continue to conduct follow-up visits and perform independent testing to verify the effectiveness of Livermore's corrective actions.

In summary, I would like to say that the deficiencies at Livermore appear to be receding with a high level of management attention now. It is clear throughout the DOE management chain that the efforts to improve safeguards and security have the personal attention and support of Secretary Richardson. While not diminishing the significance of the deficiencies identified by my inspectors, our follow-up efforts indicate that corrective actions are being taken to address the vulnerabilities that we have identified.

As I previously stated on July 1, this has not always been the case in our experience at the Department of Energy. We have seen countless reports, including many of ours, where plans and corrective actions were made with little effect. But we believe Secretary Richardson has made and continues to make a significant difference. He is a Secretary who is completely engaged. This is why we are confident that corrective actions will now be taken.

However, I assure you that the Office of Independent Oversight will continue to follow up and make certain that these corrective actions are effective. And as I stated in the July 1 briefing, we will trust but we will continue to verify. Thank you, Mr. Chairman.

[The prepared statement of Glenn S. Podonsky follows:]

PREPARED STATEMENT OF GLENN S. PODONSKY, OFFICE OF OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE, DEPARTMENT OF ENERGY

Thank you Mr. Chairman. I appreciate the opportunity to again appear before this committee to discuss the recent Office of Independent Oversight inspection of the Lawrence Livermore National Laboratory.

I am the Director of the newly created Office of Independent Oversight and Performance Assurance. As you know, we provided a classified briefing to members of this committee on July 1st on the results of our May 1999 inspection of safeguards and security programs at the Livermore National Laboratory. At that briefing, we provided copies of the inspection report to the Committee.

At this time, I would like to introduce Ms. Barbara Stone, Director of the Office of Security Evaluations. Ms. Stone was unable to attend the July 1st briefing as she was away on a much-needed vacation. At that briefing, Mr. John Hyndman provided some details on the Livermore inspection results. Mr. Hyndman is now engaged in

an inspection of Sandia National Laboratories as part of our ongoing effort to review all three of the major weapons laboratories.

For the benefit of those who were unable to attend the July 1st briefing, I would like to provide some background on who we are. My office is responsible for providing the Secretary an independent, impartial view of the effectiveness of Safeguards and Security, Cyber Security, and Emergency Management policies and programs throughout the Department of Energy. The Office of Security Evaluations performed the inspection of the Livermore Laboratory. It is one of three offices that report to me. As you may recall, the Office of Security Evaluations was originally established in 1984 to provide the Energy Department an independent assessment of the effectiveness of Safeguards and Security policies and programs throughout the Department. Congressman Dingell and Congressman Bliley were instrumental in the formation of this office. As part of Secretary Richardson's recent efforts to strengthen independent oversight of safeguards and security, the Office of Independent Oversight and Performance Assurance has been elevated to report directly to the Secretary.

Now, I will take just a minute to provide an *unclassified* summary of the results of the May Livermore inspection. Our overall conclusion was that improvements were being made at Livermore, but that significant weaknesses remain to be addressed. For example, we saw improvements in the intrusion detection systems and significant progress to improve the security of classified information on computer systems. However, we identified weaknesses that warrant continuous attention in a number of areas. One of the weaknesses involved inadequate vulnerability assessments of the Superblock, which is the area at Livermore where special nuclear material is used and stored. We also noted weaknesses in some aspects of Livermore's ability to accurately measure some types of nuclear materials. Other weaknesses were evident in Livermore's programs for protecting classified and sensitive information. We identified weaknesses in the methods for storage of classified parts and in some of the controls on access to areas containing classified matter. We were also concerned about foreign nationals being able to access Livermore's unclassified computers through dial up access. We noted that some aspects of the "nine-point" plan, which is a DOE plan for improving security of classified information, required work.

Let me emphasize that these weaknesses warrant significant attention and require prompt action. However, as I told you during the briefing on July 1st, we believe that the responsible line managers, which include the Office of Defense Programs, the Oakland Operations Office, and, and the Lawrence Livermore National Laboratory contractor management team, are taking the inspection report seriously.

Although the formal inspection ended in May, the Office of Independent Oversight has continued to follow-up on the progress to address identified deficiencies. We have been in frequent contact with the responsible DOE and Livermore managers since the inspection ended. Our follow-up efforts indicate that corrective actions are underway. For example, at the time of our July 1st briefing to this committee, and as part of our follow-up efforts, my office sent our inspectors back to Livermore to review progress at the Superblock in the areas of modeling and testing, which is needed to verify the effectiveness of the protection strategy and response plan at Livermore. Since the May 1999 inspection, Livermore has developed and is implementing a program of testing and modeling that is appropriate for verifying the effectiveness of the protective force response. Livermore also has placed additional protective force personnel in the Superblock to improve response capability until the new protection strategy is determined.

The Office of Independent Oversight will continue to conduct follow-up visits and perform independent testing to verify the effectiveness of Livermore's corrective actions.

In closing, I would like to say that the deficiencies at Livermore appear to be receiving a high level of management attention. It is clear throughout the DOE management chain that the efforts to improve safeguards and security have the personal attention and support of Secretary Richardson. While not diminishing the significance of the deficiencies identified in our report, our follow-up efforts indicate that corrective actions are being taken on the vulnerabilities we have identified. As I have previously stated, this has not always been the case in our experiences with the Department. We have seen countless reports, including many of ours, where commitment, plans, and corrective actions were made with little results. But, we believe Secretary Richardson has made, and continues to make, a significant difference. He is a Secretary who is completely engaged. This is why we have confidence that corrective actions will be taken. However, I assure you that the Office of Independent Oversight will continue to follow-up to make certain that the corrective actions are effective. As I indicted at the July 1st briefing, we will trust, but we will verify.

Thank you again Mr. Chairman, we are now ready for your questions.

Mr. UPTON. Dr. Tarter—by the way, Mr. Podonsky, we did want to receive copies of your testimony in advance. Would it be possible maybe for one of our clerks to get a copy of your opening remarks there, and we will make copies for members here in time for the questions. Could someone maybe do that for me?

TESTIMONY OF C. BRUCE TARTER

Mr. TARTER. Thank you, Mr. Chairman. Let me begin with a brief statement which is, I think, part of the opening page in my testimony. But, as I think all of you know, we are a national security laboratory. Nearly all of the work of the laboratory is focused on national security. And my particular highest responsibility each year is to certify certainly to the President of the United States that the United States stockpile of nuclear weapons is safe and reliable. That is the focus of the laboratory. And obviously being able to carry out operations in a safe and secure manner is an essential ingredient in making that annual certification to the President which we have now been able to make—this year will be the fourth year we have formally made that recommendation on the weapons in our stockpile.

To do that, we have three kinds of security at the laboratory. There is physical security, there is cybersecurity, and there is essentially what I would call personnel security. And I think the OSE evaluation focused primarily on physical security and cybersecurity, and I will make a comment or two about those, and then I will also make an additional comment about personnel security, which I think is equally important but is not the specific subject of the OSE evaluation.

In physical security, I think the area which Mr. Podonsky has mentioned of greatest concern, and I think to some degree of greatest difficulty, is that involving the guarding of special nuclear materials. And I think in all of these areas in physical security and cybersecurity as well as the personnel security, three factors come into play. One, the threat changes. The threat evolves. And I think one of the major features of the annual OSE evaluation is not to review the same set of issues each year, but to engage the threat as it's evolving and also technology as it's evolving in order to meet that threat.

In the area of physical security, I think, as Mr. Podonsky indicated, that we are focused very well on a plan involving a higher level of technology to provide the assurances and simulations to guarantee the safety of the special nuclear materials. And I think that plan—he described it both in your previous hearing, and we are in an iterative process with the Department to assure that we will reach closure on that in the near future.

In the area of cybersecurity—and I have testified to this in several other hearings in the past months—I think it is a complicated area for the U.S. Government. And I think Dr. Weigand may in his own testimony—Dr. Weigand is a particular expert in this area—make additional comments. This is not a simple thing, whether you are the Bank of America, a national security laboratory, or perhaps even Congress.

Technology is evolving very rapidly, and I think this is a complex area.

I believe you, Mr. Klink, asked about our commitment. My commitment in the area of cybersecurity goes beyond that needed to simply satisfy the OSE evaluation. I think because of the high reliance on cyberwork in our programmatic work, as well as its high vulnerability as part of intrinsic security, I am committed to not just passing the bar, but passing it with a significant gap. I think we have to do much better and I think we have begun to be engaged with the other pieces of the U.S. Government, the National Security Administration, the Department of Defense and other areas to try to make the best technology fit into cybersecurity.

Let me remind the committee of one issue which has been brought out in the evaluations, but just again to reemphasize—at Livermore, as is true at other national security laboratories, there are two kinds of computers and computer networks. There is a classified computer network in which almost all of the national security work is done, the design of bombs, the assessment of nuclear intelligence from other countries, all of those issues. And that computer system has no electronic links to any of the unclassified computer systems. It can't get there. There is an air gap as big as between your desk and mine. There is no way to transmit information between those two systems.

In the area of cybersecurity we have, I think on our own but also as a result of the Secretary's strong emphasis in this area, reinforced the security of the classified network and all of the classified computing.

In addition, I think we have as part of the 9-point plan, as part of the additional measures we have taken, we have taken a number of steps to enhance even further the general security of the unclassified computer networks. Again, as I think all of you know, that is not a technologically simple exercise to do. And I think Dr. Weigand may wish to comment on that, but I think we are putting major resources and major effort into the technology and the interactions necessary to accomplish that.

The third piece of security at the laboratory involves personnel security. And this is a matter of basically having the people who work at the laboratory and national security be reliable and be trusted people. Now, that is not the job of the laboratory, that is the job of the Department of Energy to clear them at the proper level. But it is the job of the laboratory to basically have a counterintelligence program which assesses threats, assesses interactions, and makes recommendations on how we can best both train the employees, train the system to sense vulnerabilities and to sense the threat, and the whole variety of issues that come under the word "counterintelligence."

I believe at our laboratory—and it has been put into the record in testimony not by people from the laboratory but by people from the Department—that we have an excellent, an outstanding at some levels, counterintelligence program. And I think in many respects, ensuring that that program is on a par with the best in the world is equally important to the physical and the cybersecurity. And I think we have spent a great deal of time in the two standdowns, security immersion things in training and educating

the people on a threat, on the vulnerabilities, which both because of technology and because of the evolving world general political structure, are very, very different than they were in 1985 or 1990; and that, I think, is why I believe the OSE inspections are a healthy thing. I think finding issues—an OSE team that could not find issues, I think wouldn't be a good OSE team. The laboratory that did not have corrective action plans to respond to those would not be an appropriate thing. To have a clean perfect record is neither testing us nor their system.

So I believe that process is a healthy process. I think the tension is a healthy tension and I think we're engaged in that process very well today. And when I made my comment about commitment, I think the commitment again is not this year, or other years, simply now to pass the bar but to pass the bar with a sufficient measure, a gap that in fact it will provide confidence in the Congress as well as in the Department that in fact the laboratory and its facilities are secure. Thank you very much Mr. Chairman.

[The prepared statement of C. Bruce Tarter follows:]

PREPARED STATEMENT OF C. BRUCE TARTER, DIRECTOR, LAWRENCE LIVERMORE NATIONAL LABORATORY, UNIVERSITY OF CALIFORNIA

OPENING REMARKS

Mr. Chairman and members of the committee, I am the Director of the Lawrence Livermore National Laboratory (LLNL). Our Laboratory was founded in 1952 as a nuclear weapons laboratory, and national security continues to be our central mission. Livermore is a principal participant in the Department of Energy's Stockpile Stewardship Program, heavily involved in programs to prevent the proliferation of weapons of mass destruction, and engaged in energy, environmental, and bioscience R&D as well as industrial applications of our core technologies.

Our National Security mission and safeguards and security are inextricably linked, and we take both of them very seriously at Livermore. We cannot carry out our National Security mission effectively without appropriate protection of classified and sensitive information and materials. Like National Security, safeguards and security continues to evolve in terms of requirements and objectives. We have an extensive security and counterintelligence infrastructure in place at our Laboratory, and we continually make adjustments and upgrades to address new threats and concerns. Through a process of internal self-assessments, technical consultants, and external reviews, we ensure our readiness to deal with a broad spectrum of threats. At Livermore, we believe our Special Nuclear Materials (SNM) and sensitive and classified information are secure.

The review recently conducted by the Office of Security Evaluations (OSE) was helpful in identifying areas for improvement. The OSE concluded that in two key areas, Physical Security which deals with the technical systems that help protect Special Nuclear Material, and Classified Cyber Security, which deals with the protection of our classified computing networks, the Laboratory received the highest possible rating.

That is not to say we do not have work to do. Opportunities for improvement were noted in all areas of the OSE report, and the Laboratory is firmly committed to addressing them. I would like to assure you that the concerns raised in the OSE report are receiving high priority, and resources are being made available by the Laboratory to address them.

We have invested heavily in enhanced employee training in security at Livermore. In April, we underwent an intensive two-day cyber security stand-down in which we addressed not only cyber security, but also conducted formal sessions on general security requirements and counterintelligence. In June, in response to Secretary Richardson's 5-point Security Immersion Program, we ceased all normal operations for two additional days of security training. Our employees were fully engaged in these training programs, and have made many suggestions for further improving security.

One concern raised by the OSE team had to do with the mixed Q and L clearance environment in the Limited Area of the Laboratory. In recent years, DOE's goal has been to reduce the number of Q clearances. This has been accompanied by an increase in the number of individuals having an L clearance. These are individuals

who are allowed physical access to the Limited Area but who do not have access to weapons data. For the record, I would like to note that there are no foreign nationals at LLNL with an L clearance. Any LLNL foreign national visiting the Limited Areas has always required an escort. Within the Limited Area, we rely largely on administrative controls to prohibit access to classified information by L-cleared personnel. We believe that, although well intended, the reduction in Q clearances has lessened security, and we would like to see funding made available for Q-clearances for all personnel requiring access to the Limited Area of the Laboratory.

The Annual Report to the President on Safeguards and Security rated LLNL "Unsatisfactory" in the area of Materials Control and Accountability (MC&A) and "Marginal" overall. More recently, the April/May OSE Inspection rated LLNL "Marginal" in this MC&A area. In a letter to Assistant Secretary Vic Reis dated May 14, 1999, I personally assured him that the Laboratory was committed to rectifying the rating in MC&A before the end of the calendar year. I would like to note that we are on schedule in our action plan, with most actions already complete. Similarly, in that same letter to Dr. Reis, I committed to funding and implementing the LLNL Tri-Lab INFOSEC Action Plan as approved by DOE. Again, many actions have already been completed and we continue to be on schedule. I note these formal commitments in that they also address some of the concerns raised in the OSE evaluation.

The OSE team was careful to note in their report major improvements made in the Safeguards and Security program to address past concerns, and these improvements are continuing. There have been important technical upgrades to the Perimeter Intrusion Detection and Alarm System (PIDAS) that surrounds our Superblock, which contains our Plutonium facility, to provide early detection of both airborne and bridging attacks. We have recruited and put in place an offensively trained Special Response Team having the training necessary to implement a recovery or recapture action. One hundred percent searches are conducted at material access area portals in the Plutonium Facility. Over 100 simulations of adversary attacks have been completed, and we are continuing to refine our simulation methodology, attack scenarios, and defensive strategies. We have engaged an external advisory group of very senior former military and FBI experts to advise us in this work. Since the completion of the OSE SE we have committed additional officers to the Superblock and taken other compensatory measures to assure the security of our SNM assets.

Other improvements noted in the OSE report include the installation of an intrusion detection system in a building inside the Limited Area used for the storage of classified non-SNM weapons parts. Alarm systems are now in design for two other facilities in the Limited Area. Foreign Ownership, Control or Influence (FOCI) reviews of all contractors have been completed. A baseline inventory of plutonium has been completed, and improved procedures to ensure effective and timely accounting for any inventory differences have been put in place.

In the area of cyber security, we have already implemented many elements of the Tri-Lab Committee's "nine point plan." For example, steps have been taken to ensure the physical incompatibility of removable media between classified and nearby unclassified computer systems. Scanning of outgoing e-mail has been instituted, and funding has been committed for implementation of a multi-level system that will separate sensitive unclassified computer processing from the remainder of unclassified processing. The frequency of vulnerability scans of network computers is being increased, and unclassified archives are being scanned for classified content. To date over 4 million files have been scanned, and no classified content has been found. Procedures for authorizing access to unclassified computers by foreign nationals have been tightened, and today no foreign nationals have access to Livermore unclassified computer networks without having gone through an indices check and having a formal computer security plan approved by the Laboratory. All dial-up access by foreign nationals is routed through a common terminal server which has special intrusion detection software.

In summary, safeguards and security go hand in hand with our National Security mission at Livermore. We are committed to an excellent safeguards and security program, and have been taking, and will continue to take, the steps necessary to achieve it.

PHYSICAL SECURITY AT LIVERMORE

Livermore's security construct is based on a series of defensive layers—a graded approach that provides increasing barriers that correspond to the increasing value of critical Laboratory assets.

Clearances, badging, and background checks on Laboratory employees (including subcontractors) constitute a first line of defense. Those people with access to classified assets undergo background investigations associated with DOE Q, L or sen-

sitive compartmented information (SCI) clearances as appropriate. Reinvestigations are scheduled automatically at five-year intervals or as needed on a for-cause basis.

Livermore uses a defense-in-depth approach to physical barriers—fences, doors, repositories, and vaults. The Laboratory's outer perimeter fence provides the basic physical protection to U.S. government property. Additional protection is provided for "limited" areas where classified assets are present. The level of clearance required to freely transit these areas is also higher. Classified parts and materials are provided additional physical protection and access control. Significant quantities of special nuclear material receive the highest level of protection, with vault-like physical protection as well as aggressive armed defense and response capabilities.

At each physical barrier (e.g., fence, building, vault), there are various levels of access control. Access control is performed either by security officers or automated security access portals. At more restricted areas, access is checked against specific access lists. Need-to-know is required, in addition to the appropriate clearance, before an individual is allowed access to classified assets.

The Laboratory employs security officers who are fully trained and accredited to meet DOE criteria. The level of training varies with the assignment (defensive, offensive, or special response). We currently have over 40 offensively trained officers in our Special Response Team and have a new group beginning academy training next month. Training is extensive and performance based. The security force undergoes regular performance tests, self-assessments, DOE surveillance, and inspections.

Physical security is designed into new facilities and facility modifications. Detection systems are continuously monitored and routinely tested. The Laboratory's security system is prepared for armed response to all unauthorized intrusions.

In the Annual Report to the President on Safeguards and Security we received a "Marginal" rating overall but, an "Unsatisfactory" rating in MC&A. The issue involved our inability to meet SNM inventory requirements at a time when the Plutonium Facility was shut down to address safety concerns, preventing monitoring and measurements. Now that safety concerns have been addressed and the facility reopened, we have resumed all special nuclear material measurements and inventory monitoring and we believe we will be in compliance with DOE requirements.

We have high confidence in our Safeguards and Security programs and in the security of our critical assets. We have implemented technical and procedural enhancements to strengthen our physical security, remedied material control and accounting deficiencies, and fully upgraded our strategy to protect nuclear material at our Laboratory.

CYBER SECURITY AT LIVERMORE

Cyber or computer security is a critical element of Livermore's overall security construct. The Laboratory has both classified computer networks and unclassified computer networks. The two are separate and are not connected. We also have numerous stand-alone computer systems and local area networks in both classified and unclassified areas. There are no connections from Livermore's classified computers to the outside world except through NSA-approved encryption.

In addition to physical barriers between the unclassified and classified computing environments at Livermore, there are need-to-know barriers within the classified computer systems. Access to a classified computing network does not grant users access to all the information in that network. The same need-to-know requirements that apply to verbally communicated information and documents also apply to computer-stored information.

Recent concerns about espionage involving computer-based information and codes spurred a thorough reassessment of computer security at our Laboratory, including threat awareness and training. We support the Secretary of Energy's cyber security initiative and are contributing to his INFOSEC planning.

On April 2, 1999, the Secretary of Energy called for a stand-down of all classified computing at the three DOE national security laboratories. At Livermore, we went even further and shut down all classified computing, all co-located unclassified computing, and all unclassified supercomputing. The stand-down was the first step of a Tri-Lab INFOSEC Action Plan that has been developed and approved by Secretary Richardson. The plan consists of nine action items with specific scheduled milestones. We have met all milestones to date. We will continue working with the DOE Office of Chief Information Officer (CIO) to fully implement the Tri-Lab INFOSEC Action Plan and further enhance cyber security at the Laboratory.

In addition, on June 21-22, we conducted a two-day-long Security Immersion Program at Livermore to accelerate the security initiatives launched by Secretary Richardson in April. Supervisors were instructed to ensure that all Laboratory employees complete the program, which was directed toward five objectives identified by

the Secretary to strengthen security at the laboratories, assessing security issues in individual work areas, and applying what has been learned to each individual's workplace.

We have taken dramatic steps to focus the attention of all Laboratory employees on the threat of foreign intelligence sources as related to cyber security. All employees (including those who do not normally use computers but could have need or access in the future) received special computer security training. We also trained subcontractor employees and consultants. All computing was discontinued until training was complete for all employees on site. Employees who were on travel or leave were trained immediately upon their return. In addition, we have since expanded our on-going computer security training and threat awareness training for all Laboratory personnel using classified computers. This training is unclassified and accessible via a website to make it readily available to our employees and easy to update.

Every computer work area and environment at Livermore was evaluated and changes were made as necessary to ensure that LLNL classified and sensitive computing meet the highest standards of information security. In particular:

- We have also taken measures to preclude the transfer of information from classified to unclassified computers in a single work area by the use of removable media.
- We have instituted two-person controls over the authorized transfer of unclassified information from classified computers to unclassified computers.
- Until a more permanent security fix is in place, since April 2, 1999, we have temporarily disabled the file interchange system on the classified supercomputer so that it is impossible to transfer files from the classified supercomputers or the archives to an unclassified computer.
- We also have begun to scan outgoing presumably unclassified e-mail as well as computer files for possible sensitive or classified information. To date, we have scanned over 4 million files in our effort to ensure there is no classified material in unclassified computer files. No issues have arisen.
- We have strong need-to-know controls on our classified network; yet we are investigating ways to provide an even greater level of protection. We are also studying how to apply these same concepts to the unclassified systems to provide better protection to unclassified sensitive information.

In addition, I have also created a Computer Security Policy Board comprised of senior managers to both develop policies and advise me on matters related to unclassified computer security. (Classified computer security policy is defined by DOE Orders.)

On our unclassified computing network, we are improving the way we protect unclassified sensitive information. Some information must be available worldwide, but other information must be protected for privacy, proprietary, or export control reasons. We are implementing additional "firewalls" within our unclassified network to separate fully accessible information from unclassified sensitive information. For several years, Livermore has had an ongoing program to annually scan/audit a subset of its unclassified computer systems for security vulnerabilities. We have expanded this policy so that now all unclassified computer systems must be scanned at least once a year and that appropriate correction/fixes to detect vulnerabilities must be undertaken immediately.

The Laboratory has long had a policy of monitoring users accessing our computer resources via the Internet. We have now expanded our monitoring to cover all dial in access to Livermore computers. Any Foreign Nationals (FNs) with dial-in capabilities are monitored. Additionally, any FN granted access to unclassified computer resources must first have a programmatic justification of need by the sponsoring Laboratory program and an approved security plan on record for each FN. The Laboratory required that all FNs with access to computer resources had to be recertified by June 30, 1999. No one was "grandfathered" in under our process and those not recertified are being denied access to the computer resources. Certification refers to having a programmatic justification and a security plan in place. Livermore will require that all FNs granted access to Laboratory computer resources must be processed through the Foreign Visits and Assignments Office. This will ensure that any FN with access to Laboratory computer resources will have met the necessary criteria and that their access to computer resources is being monitored.

Finally, our Laboratory is working with personnel at Sandia, Los Alamos, and DOE to develop a "best in practice" plan for cyber security. So far, we have completed a benchmarking of several organizations inside and outside of the government to determine what others are doing to protect information from both outsiders and insiders. This planning activity has an oversight board that is currently being staffed with cyber security professionals from industry along with the CIOs from the three laboratories.

Our approach to cyber security goes beyond addressing vulnerabilities or problems that we identify or that are brought to our attention. We are using this cyber security upgrade as an opportunity to apply our multi-disciplinary approach to science and technology to become a model for cyber security. Leading-edge cyber security is vital to our programmatic missions and is an area where we can leverage our expertise to enhance national security in the broadest sense.

CLOSING REMARKS

Accomplishing our national security mission requires outstanding science and technology. Simultaneously, we must ensure that the application of that science and technology to national security is protected at all levels. We have long recognized the inherent challenge involved in protecting national security information while fostering the interchange of ideas required for cutting-edge science and technology. Indeed, to a considerable degree, the nation's security rests on the technological advances that arise from the world-class R&D conducted at Livermore and the other national security laboratories.

A multi-faceted security apparatus is in place at our Laboratory, including physical security, operational security, personnel security, information security, communications security, cyber security, counterintelligence, and employee security awareness. We continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on security and counterintelligence issues, whether they are anticipated or identified by us or others, or are brought to our attention in the form of executive or departmental orders or inspections. Proactive and effective security and counterintelligence allows us to meet the challenge of ensuring national security while operating in a global world.The recent evaluation conducted by OSE noted many improvements to LLNL's security system while identifying areas for further improvement. We have prepared an aggressive corrective action plan that, technology permitting, will resolve any issues by the end of the year. I have committed the resources and established the priority to ensure that this plan is executed. Corrective actions have already been taken on many issues and, as appropriate, compensatory actions are in place. I am confident that at LLNL, our Special Nuclear Material and sensitive and classified information are secure.

Mr. UPTON. Thank you. Dr. Weigand, would you like to comment?

STATEMENT OF GIL WEIGAND

Mr. WEIGAND. I will make a set of very brief comments. I would like to give you the opportunity to ask me any questions that you would like.

Good morning, Mr. Chairman, and subcommittee members. I am Dr. Gil Weigand. I am the Deputy Assistant Secretary for Research Development Simulation and Defense Programs. That is a slightly different title than you utilized. We are in the process of reorganization, as you are well aware, trying to define line management a little bit better, and two organizations have been combined and now I am responsible. I have been in this position for 8 months and this position is responsible for the laboratories.

I was put in this position because I bring to that position industry and DOD program management experience. As I indicated in the July 1 testimony to the subcommittee, Defense Programs recognizes that our job is to fix the problems. We agree substantially with the issues identified by Mr. Podonsky and his team and have taken both immediate and interim actions to address their concerns. I want to point out that since taking this position in this area that involves Livermore and the security, I have put in place no less than four corrective action plans. And those corrective action plans have milestones that have weekly or monthly obligations by the laboratory, and to date the laboratory has not missed a single one of them.

I also, when finding out the results from Mr. Podonsky, before he even left the site we were in the process of doing what I call a path forward plan, which was an immediate layout of the plan that ultimately became part of the broader planning for corrective action on this in the area of special nuclear materials. It is extremely important that we protect those materials, but it is also extremely important that I have those facilities available and open to me, since I am equally responsible now for the facilities and for the conduct of the research and development at the laboratories. A draft of that plan, by the way, has been reviewed by Mr. Podonsky's team and we have incorporated their comments.

As a result of the cybersecurity concerns, we directed the formation of a cybersecurity integrated security management plan. The first step is the development of a plan by August 1 which will create the most aggressive, across-the-board advance in cybersecurity at the labs. Not on my account. That will not be me that is basically saying that, but by the account of some of the Nation's foremost experts in cybersecurity.

The management team is headed by Bill Crowell, former deputy director of NSA. Last the Department, at the direction of Secretary Moniz, have taken parts of the corrective action plans that we have created and incorporated those into the Department's goalposts plan which will result in a green designation for safeguards and security at LLNL, the Livermore labs, by the end of the year.

As you recall, Mr. Chairman, Bill Hensley and I briefed you in the last hearing on some of those actions and we will be happy to more extensively amplify on those in the closed session. The detailed are classified.

Since the July 1 hearing, the corrective action plan has been finalized, with specific milestones assuring the concerns identified by Mr. Podonsky are appropriately addressed by the end of the calendar year. Since I now have a completed and corrective action plan, I intend to also implement some measures by which there is accountability. And I intend to hold both Federal managers accountable and laboratory managers accountable.

In addition to that, I have directed that there be the creation of a tracking system to specifically track each issue as corrective actions and associated milestones are completed or not completed. Mr. Hensley, who directs our security office at Defense Programs, has created three viewgraphs that we will take up with you in later session. They are very brief, but we wanted to give you a status of where we stand.

Thank you very much for the opportunity to provide you with another update on the progress of security, and I am available for questions.

[The prepared statement of Gil Weigand follows:]

PREPARED STATEMENT OF GIL WEIGAND, DEPUTY ASSISTANT SECRETARY FOR RESEARCH, DEVELOPMENT AND SIMULATION AT DEFENSE PROGRAMS, DEPARTMENT OF ENERGY

Good morning Mr. Chairman and Subcommittee Members: I am Dr. Gil Weigand, I am the Deputy Assistant Secretary for Research, Development and Simulation at Defense Programs. I have been in this current position for about 8 months. I was put in this position because I would bring to this position industry and DoD program management experience.

As I indicated during the July 1, 1999 testimony to the Subcommittee, Defense Programs (DP) recognizes that our job is "TO FIX THE PROBLEMS." We agree substantially with the issues identified by Mr. Podonsky and his team and have both immediate and interim actions to address their concerns. I have directed that a corrective action plan in general for safeguards and a path-forward plan specifically for the special nuclear material areas be developed which addresses each of the concerns in Mr. Podonsky team's findings. A draft of that plan has been reviewed by Mr. Podonsky's team and we have incorporated their comments. Furthermore, as a result of cyber-security concerns, I directed the formation of a cyber-security integrated security management plan. The first step is the development of a plan by August 1 which will create the most aggressive across the board advance in cybersecurity at the labs, not by my account, but by the account of some of the nations foremost experts in cybersecurity. The management team is headed by Bill Crowell, former Deputy Director of NSA. Lastly, the department under the direction of Undersecretary Moniz we have created plans, the Department's Goal Posts Plan, which will result in a "green" designation for safeguards and security at LLNL by the end of the year. As you will recall, Mr. Hensley and I briefed you during the last Hearing on some of those actions.

Since the July 1, 1999 Hearing, the corrective action plan has been finalized with specific milestones for assuring the concerns identified by Mr. Podonsky are appropriately addressed by the end of the calendar year. A tracking system is being developed to specifically track each issue, its corrective action(s), and associated milestones.

Mr. Hensley who directs the security office at Defense Programs will conclude our time here by providing you with a three slide summary of the corrective action plan's status. We will provide for the record the classified detailed corrective action briefing.

Thank you very much for the opportunity to provide you with another update on our progress in security. Mr. Hensley please provide the committee with you status report.

Mr. UPTON. Thank you. Dr. Turner, do you have something you would like to add?

STATEMENT OF JAMES TURNER

Mr. TURNER. Yes, sir, I do. I appreciate the opportunity to be here. I would like to start with some summary statements and then step back from that to give you a quick overview of our role as a field element.

First of all, back in April, Bruce and I, along with some others, were involved in a video teleconference with the Secretary. At that time I gave him my personal assurance that we would do everything that was necessary to correct the items that were found in the 1998 Report to the President, as well as the things that Glenn's team came up with.

I saw the Secretary last week at an event and personally reiterated my assurance. I spent part of last week going over the issues regarding storage of classified parts. We were briefed on the upgrades to the alarm system that was being put in place, as well as continuously tracking the corrective action plan. All the items are on track in that corrective action plan. They are being completed on time. And I think this represents a commitment from all of us at the table to make that happen.

That being said, let me step back for a moment and talk about our role and responsibility as a field element and the team that we have here today. First of all, we're the contracting officer for Lawrence Livermore National Laboratory. In conjunction with headquarters, we set expectations for the laboratory in a number of areas, including security, and we assess their performance annually. We also provide Federal oversight, and in that role we have the line management function in safety and security at the lab. We

provide assurance to headquarters that not only are the provisions of the contract being met, but also DOE policy objectives are being met by the laboratory.

In the implementation of that security role, we develop an annual a site safeguards and security plan which provides a protection strategy for the laboratory as well as specific performance measures in the contract on which the laboratory is graded. We have an onsite presence which means that on a daily basis people are walking through the facilities, checking things and looking at how things are being done to understand what the laboratory is doing. And, on occasion when it is necessary, there are findings and concerns that are developed out of that but it also provides us a direct way to track and validate that corrective actions are in fact being done.

There is an annual survey report which summaries of these daily operational awareness activities. The report goes into the contract assessment as well as inputs provided to headquarters. We, in turn, are overseen by headquarters. Defense programs is our boss for everything that goes on at Livermore. That is very clear to us. We have a management agreement that has been signed with Gil Weigand, and there is also another document that has been signed which has been presented to Vic Reis for signature that spells out roles and responsibilities for our office and defense programs.

We also appreciate the input from the Office of Security Evaluations, Glenn's office, because they provide us with increased confidence in what we're doing and what we're finding. They also share with us their experience from other parts of the complex. They see the whole picture while we only see a part of it, and it is best practices that we can incorporate.

We have reported on some progress at the July 1 briefing. Since then, there has been additional progress. Glenn talked about the progress that's been made in the protection strategy for Superblock. Also, the laboratory has completed the second of three bimonthly inventories for materials control and accountability. We wanted them to complete three before we would go back and look at our evaluation. They are also upgrading the alarm systems for the storage of classified parts.

As far as my role is concerned, I am a physicist. I have been at Oakland for 5 years. I have been the manager there for 4 years. Prior to going to Oakland, I was the director of the Defense Programs Office of Nuclear Weapons Security, and in that capacity I had the responsibility for safety, security and use control. So for me, it is more than an intellectual exercise, it is something that I feel, something I live and something I sincerely believe.

I am out at Livermore at least 1 day a week. We have weekly meetings with our site manager where we talk about what is his assessment of how we're moving on the corrective action plan. I meet once a week with Livermore senior management and we discuss security—an item on that agenda is always the corrective action plan.

Again, speaking for the office, I will give my personal assurance to the Secretary as well as provide it to you, that we will do the things that are necessary to get the lab green or satisfactory by the end of the year.

I would also like to take the opportunity to introduce the members of our team that are here today. First of all, Marty Domagala, our Deputy Manager is here. He led the team that came back for the July 1 briefing. Jim Hirahara, our Assistant Manager for Operations and Safe Management. One of his responsibilities is the University of California contract. I understand there were some questions that came up the last time about that. And also Rich Mortensen, our Director of Safeguards Security. With that, I am happy to answer any questions that you may have.

Mr. UPTON. Terrific. Having completed our witnesses' public statements, the Chair will recognize himself for a unanimous consent request and to offer a motion.

Mr. STUPAK. Mr. Chairman, before we do that, I hate to interrupt you, but Dr. Weigand and Dr. Turner both had statements before them. We never received copies of those. Could we get copies of those statements I would like to look at the in the future?

Mr. WEIGAND. Absolutely. I was not asked to provide—and I apologize for not thinking forward on that.

Mr. TURNER. I was under the understanding that an oral statement—but we will certainly provide.

Mr. UPTON. Terrific. Thank you. Without objection, staff of the majority—my motion is this: Without objection, staff of the majority and minority parties may be recognized to question witnesses for equal 30 minute blocks pursuant to clause 2(j) of rule XI of the Rules of the House. Is there objection? Hearing none.

Mr. BARTON. Mr. Chairman?

Mr. UPTON. The gentleman is recognized.

Mr. BARTON. You want the staff to question the witnesses in this hearing or later on?

Mr. UPTON. Later on. It will be part of the hearing.

Hearing none, so ordered.

Further, the Chair moves that pursuant to clause 2(g) of Rule XI, the Rules of the House, the remainder of this hearing to conducted in executive session to protect information that might endanger national security. Is there discussion on the motion? If there is no discussion, pursuant to the rule, a recorded vote is ordered.

All in favor of moving to executive session will indicate by saying aye.

Opposed, say nay.

The Clerk will call the roll.

The CLERK. Mr. Barton.

Mr. BARTON. Yes.

The CLERK. Mr. Barton votes aye.

Mr. Cox.

[No response.]

The CLERK. Mr. Burr.

Mr. BURR. Aye.

The CLERK. Mr. Burr votes aye.

Mr. Bilbray.

Mr. BILBRAY. Aye.

The CLERK. Mr. Bilbray votes aye.

Mr. Whitfield.

[No response.]

The CLERK. Mr. Ganske.

Mr. GANSKE. Aye.
The CLERK. Mr. Ganske votes aye.
Mr. Blunt.
[No response.]
The CLERK. Mr. Bryant.
Mr. BRYANT. Aye.
The CLERK. Mr. Bryant votes aye.
Mr. Bliley.
[No response.]
The CLERK. Mr. Klink.
Mr. KLINK. Aye.
The CLERK. Mr. Klink votes aye.
Mr. Waxman.
[No response.]
The CLERK. Mr. Stupak.
Mr. STUPAK. No.
The CLERK. Mr. Stupak votes no.
Mr. Green.
[No response.]
The CLERK. Ms. McCarthy.
Ms. MCCARTHY. Aye.
The CLERK. Ms. McCarthy votes aye.
Mr. Strickland.
Mr. STRICKLAND. No.
The CLERK. Mr. Strickland votes no.
Ms. DeGette.
Ms. DEGETTE. Aye.
The CLERK. Ms. DeGette votes aye.
Mr. Dingell.
[No response.]
The CLERK. Mr. Upton.
Mr. UPTON. Aye.
The CLERK. Mr. Upton votes aye.
Mr. UPTON. The Clerk will report the result.
The CLERK. Mr. Chairman, on that vote there were 9 ayes, 2 noes.

Mr. UPTON. Members having voted in the affirmative and a quorum being present, the motion is agreed to. Accordingly, the Chair declares the subcommittee in recess subject to the call of the Chair, pending which all members, staff, witnesses, and guests will leave the room.

The Capitol Police at this point will secure the room and I would note that we will come back at 11:05 for members that are going to be able to come back.

[Whereupon, at 10:45 a.m., the subcommittee recessed. To reconvene at 11:05 a.m. executive session.]