

**THE STATE OF SECURITY AT THE DEPARTMENT
OF ENERGY'S NUCLEAR WEAPON LABORATORIES**

HEARING
BEFORE THE
SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS
OF THE
COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
FIRST SESSION

—————
OCTOBER 26, 1999
—————

Serial No. 106-103
—————

Printed for the use of the Committee on Commerce



U.S. GOVERNMENT PRINTING OFFICE

61-036CC

WASHINGTON : 2000

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana	JOHN D. DINGELL, Michigan
MICHAEL G. OXLEY, Ohio	HENRY A. WAXMAN, California
MICHAEL BILIRAKIS, Florida	EDWARD J. MARKEY, Massachusetts
JOE BARTON, Texas	RALPH M. HALL, Texas
FRED UPTON, Michigan	RICK BOUCHER, Virginia
CLIFF STEARNS, Florida	EDOLPHUS TOWNS, New York
PAUL E. GILLMOR, Ohio	FRANK PALLONE, Jr., New Jersey
<i>Vice Chairman</i>	SHERROD BROWN, Ohio
JAMES C. GREENWOOD, Pennsylvania	BART GORDON, Tennessee
CHRISTOPHER COX, California	PETER DEUTSCH, Florida
NATHAN DEAL, Georgia	BOBBY L. RUSH, Illinois
STEVE LARGENT, Oklahoma	ANNA G. ESHOO, California
RICHARD BURR, North Carolina	RON KLINK, Pennsylvania
BRIAN P. BILBRAY, California	BART STUPAK, Michigan
ED WHITFIELD, Kentucky	ELIOT L. ENGEL, New York
GREG GANSKE, Iowa	THOMAS C. SAWYER, Ohio
CHARLIE NORWOOD, Georgia	ALBERT R. WYNN, Maryland
TOM A. COBURN, Oklahoma	GENE GREEN, Texas
RICK LAZIO, New York	KAREN MCCARTHY, Missouri
BARBARA CUBIN, Wyoming	TED STRICKLAND, Ohio
JAMES E. ROGAN, California	DIANA DEGETTE, Colorado
JOHN SHIMKUS, Illinois	THOMAS M. BARRETT, Wisconsin
HEATHER WILSON, New Mexico	BILL LUTHER, Minnesota
JOHN B. SHADEGG, Arizona	LOIS CAPPS, California
CHARLES W. "CHIP" PICKERING, Mississippi	
VITO FOSSELLA, New York	
ROY BLUNT, Missouri	
ED BRYANT, Tennessee	
ROBERT L. EHRLICH, Jr., Maryland	

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	RON KLINK, Pennsylvania
CHRISTOPHER COX, California	HENRY A. WAXMAN, California
RICHARD BURR, North Carolina	BART STUPAK, Michigan
<i>Vice Chairman</i>	GENE GREEN, Texas
BRIAN P. BILBRAY, California	KAREN MCCARTHY, Missouri
ED WHITFIELD, Kentucky	TED STRICKLAND, Ohio
GREG GANSKE, Iowa	DIANA DEGETTE, Colorado
ROY BLUNT, Missouri	JOHN D. DINGELL, Michigan,
ED BRYANT, Tennessee	(Ex Officio)
TOM BLILEY, Virginia, (Ex Officio)	

CONTENTS

	Page
Testimony of:	
Browne, John C., Director, Los Alamos National Laboratory	106
Curran, Edward J., Director, Office of Counterintelligence, U.S. Department of Energy	17
Habiger, Eugene E., Director, Office of Security and Emergency Operations, U.S. Department of Energy	12
Podonsky, Glenn S., Director, Office of Independent Oversight and Performance Assurance, U.S. Department of Energy	6
Robinson, C. Paul, President and Laboratories Director, Sandia National Laboratories	50
Tarter, C. Bruce, Director, Lawrence Livermore National Laboratory	92
Turner, James, Manager, Oakland Operations Office, U.S. Department of Energy	101
Weigand, Gil, Deputy Assistant Secretary, Strategic Computing and Simulation, U.S. Department of Energy	97
Material submitted for the record by:	
Angell, John C., Assistant Secretary, Congressional and Intergovernmental Affairs, Department of Energy:	
Letter dated December 14, 1999, to Hon. Fred Upton, enclosing response for the record	140
Letter dated June 16, 2000, to Hon. Fred Upton, enclosing response for the record	212
Browne, John C., Director, Los Alamos National Laboratory, responses for the record	168
Inlow, Rush O., Deputy Manager, Albuquerque Operations Office, Department of Energy:	
Letter dated November 29, 1999, to Hon. Fred Upton	121
Letter dated December 13, 1999, to Hon. Fred Upton	126
Podonsky, Glenn S., Director, Office of Independent Oversight and Performance Assurance, U.S. Department of Energy, responses for the record	187
Robinson, C. Paul, President and Laboratories Director, Sandia National Laboratories, responses for the record	174
Tarter, C. Bruce, Director, Lawrence Livermore National Laboratory, letter dated December 13, 1999, to Hon. Fred Upton, enclosing response for the record	129
Turner, James, Manager, Oakland Operations Office, U.S. Department of Energy, responses for the record	162

THE STATE OF SECURITY AT THE DEPARTMENT OF ENERGY'S NUCLEAR WEAPON LABORATORIES

TUESDAY, OCTOBER 26, 1999

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

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2322, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Cox, Burr, Bilbray, Ganske, Bryant, Bliley, (ex officio), Stupak, and Green.

Also present: Representative Wilson.

Staff present: Tom DiLenge, majority counsel; Anthony Habib, legislative clerk; and Edith Holleman, minority counsel.

Mr. UPTON. Good morning. We are here today to conduct what will be our fourth public hearing this year to explore the critically important, and very troubling, issue of lax security at our Nation's key nuclear weapons laboratories. We will hear today from the top security advisors to Energy Secretary Bill Richardson, as well as the directors of Los Alamos, Lawrence Livermore, and Sandia National Laboratories.

In particular, we will hear from the Department's chief internal inspector, Mr. Glenn Podonsky, whose team of inspectors recently concluded inspections at Los Alamos and Sandia. Mr. Podonsky previously testified before this subcommittee on his team's inspection of Lawrence Livermore. Taken together, these three inspection reports raise serious questions about the Department's ability to effectively run a national security apparatus.

One of the most surprising, recurring findings in these reports is the lack of effective policy guidance by the Department on security matters. Given the fact that the Department has nearly 20 different security contractors or subcontractors at various sites across the country, one would think that the DOE would set clear requirements to assure some degree of nationwide consistency and some minimal level of security at each site. Yet the reality is far different.

For example, the Department has long required that the labs take certain steps to ensure that foreign visitors or assignees and not spies, and that their access to sensitive information is adequately restricted. Yet the Department's guidance seemingly applies to only those foreign nationals physically located onsite. Thus,

in the case of Lawrence Livermore for example, this policy was not applied to foreign nationals who had remote access to the lab's computers since they were not actually "onsite."

Of course, such a distinction makes little common sense—indeed, remote access may raise greater security concerns than onsite access since it is more difficult to determine whether the individual at the other end is, in fact, the authorized user. But it was not until the recent inspection by Mr. Podonsky's team that this practice was discovered and halted. The Department still has not addressed this question as a matter of policy, nor the related questions of how to deal with the other information sharing with offsite foreign nationals, including video- and tele-conferences or e-mail. Similarly, the Department has never had any policy that set minimum standards for computer password creation and use. Thus, the labs have done their own thing—in some cases, passwords were not used at all, while in other cases, passwords were common names and only a few characters in length, and often were not changed with any frequency. I find it hard to believe that this committee—which does not engage in classified computing and does not possess on its computer systems national security information—has a more stringent password controls than our Nation's nuclear weapon labs.

And the generally poor state of unclassified computer security at these labs—what Mr. Podonsky calls their numerous potentially exploitable vulnerabilities—can also be traced back to the lack of any detailed policy from the Department in this area. At two of the labs, the inspection team found that the closed lab network could be penetrated from the outside through the Internet, while all of the labs suffered from general system weaknesses that permitted users, once on the system, to move freely among data bases, gain passwords, and access sensitive information without a need to know. With literally hundreds of foreign nationals authorized on these systems, including many from sensitive countries, the risk of disclosure of sensitive nuclear information, business proprietary data, or export-controlled materials is significant and certainly worrisome.

It is ironic that a Department and laboratory management that prides itself in being on the cutting edge of research and technology has fallen so far short in this high-tech area. Indeed, Lawrence Livermore is supposed to be the Department's computer technology headquarters. It is clear that DOE policy in this area needs to be brought into the 1990's, and hopefully before we begin the next decade and get even further behind.

We will hear today about how the Department is drafting policies to deal with remote access, computer passwords, fire walls, and the potential for unauthorized transfers or downloads of classified information, such as those allegedly performed by Wen Ho Lee. Yet, with the exception of the remote access issue, these problems were identified 5 years ago by both Mr. Podonsky's office and the Office of Safeguards and Securities. The response at the time, from both the labs and the DOE hierarchy, was that computer security wasn't worth the cost and that they were willing to accept the risk. I am pleased to see that the DOE management and the labs are now beginning to change their tune, but where is the accountability for years of negligence that may have seriously compromised our na-

tional security? Secretary Richardson boasts of recommending disciplinary action against a handful of lab employees for failing to take seriously the Wen Ho Lee counterintelligence case. Yet no one in the labs has been held accountable for the years of resistance to implementing sound computer security policies.

This lack of accountability goes beyond the computer security area. We will hear today about how Los Alamos has made much progress over the last 6 months fixing a very troubling situation involving the protection of classified weapons parts—a problem that was first identified by the Department inspectors more than 5 years ago. Despite directives from the Department and agreed-upon action plans, Los Alamos failed to take any meaningful steps to correct this situation, year after year, such that the situation was essentially unchanged when the inspectors returned 3 years later in 1997. Inspections in 1998 and 1999 revealed the same problems, but this time the wave of bad publicity about lab security seems to have prompted Los Alamos to begin corrective action to protect classified weapons parts.

But did Los Alamos pay for its stubborn refusal to fix this problem? To the contrary—despite the significance of the long-standing deficiencies, Los Alamos received excellent or similarly laudatory security ratings in its annual contract performance appraisals, increasing the bonuses that its senior management received from the U.S. taxpayers.

As I said before, unless we have a rigorous annual inspection process that imposes real financial penalties on the labs for failing to comply with DOE's security requirements, I don't believe we will ever change the culture and achieve lasting security reform. The recently-passed Defense Authorization Act provides a framework for such action, but it will be up to the Department to take that authorization seriously and begin implementing serious contract and oversight reform.

I have already begun discussions with the chairman of the full committee to perhaps allow a number of us to go out early next year to visit some of the labs, and I look forward to the cooperation by the Department to make sure that will go without a hitch.

With that, I will recognize Mr. Green from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I will be brief.

Thank you for scheduling today's hearing and keeping this issue on the front burner, so to speak.

DOE has had problems for many years with regular, continued oversight. Hopefully, our subcommittee and Congress will be able to finally solve this decades-long problem. This committee is prepared to hear testimony from DOE about its plans to revamp and improve the security at our nuclear weapons laboratories. This time, I hope we will be able to see real progress on the security solutions at the Nation's labs.

I especially look forward to the testimony of Mr. Podonsky, whose inspection teams recently completed security evaluations at both Los Alamos and Sandia National Labs. I appreciate all the hard work by the inspection teams in analyzing the strengths and weaknesses of the security in these labs. Our committee needs to look for solutions to the loss of the classified information.

And, again, Mr. Chairman, thank you for holding this hearing. And, again, I appreciate the continued effort because long before we were in Congress, this was a problem. Maybe we can put this to rest and have DOE do what we need to do to protect the classified information.

Mr. UPTON. Thank you, Mr. Green.

Mr. Cox.

Mr. COX. Thank you, Mr. Chairman. I welcome our panel.

The issues that we are addressing today are issues that have been before this committee during Republican and Democratic Congresses over a period of many years and that have been the subject of examination by the executive branch in a variety of ways, also over the last several years, including specifically the 1995 Galvin task force report, a half dozen GAO reports, the report of the Select Committee that I chaired, evaluations by the Intelligence Committees of the House and the Senate. The President's Foreign Intelligence Advisory this year, the PFIAB report, said the Department of Energy has had a dysfunctional management structure and culture that only occasionally gave proper credence to the need for security and counterintelligence programs at the weapons labs. That is a conclusion that I know, at least as of last year, Mr. Curran shared because he shared that with our Select Committee.

Today, we are going to hear that DOE has finally gotten the message, that by the end of this year all of DOE's nuclear weapons labs will meet the highest security standards. Our concern, as you might expect, given this track record, is how to distinguish between these representations that everything is fine and those that we have received in the past. Over the past 5 years DOE inspectors have repeatedly identified these very same problems, but still nothing changed. Each negative report has been met with earnest announcements that finally decisive action will be taken and these problems will be resolved.

It was after these years of nonresponsiveness, including throughout 1½ terms of the Clinton administration itself, that President Clinton issued his Presidential decision Directive PDD-61, which ordered from the Presidential level counterintelligence measures at the nuclear weapons laboratories.

Mr. Curran, who is before the committee today, made 46 recommendations to implement PDD-61. Today, nearly a year later, at least 10 of those recommendations have not yet been implemented. Furthermore, some of the recommendations are worded such that the Secretary of Energy can claim implementation of a recommendation based on the issuance of an order in Washington, regardless of whether the changes were actually implemented at the labs.

I appreciate this committee's continuing attention to the protection of our scientific and military information. It is only through sustained oversight and full implementation of the reform measures that you have all identified that we will be able to secure our information in the future and perform our tasks as we are supposed to do.

I know that the history of this problem places a great burden on you as individuals. It likewise puts us in the position, as Congress, in the conduct of our oversight of Lucy, Charlie Brown and the fa-

mous football. We hope that this time what we're hearing is the truth, that—I know it has always been intended as the truth. It was intended as true as spoken, but we hope this time there will be change and follow-through, and by the end of this year, we will be in the Promised Land.

And I appreciate the time for the opening statement, Mr. Chairman. I also apologize because, as you know, I have a bill on the floor; my Internet tax bill is the second on the schedule, and it will require me to be gone for about an hour of this hearing at some undetermined time; but I am of course very interested in these subjects and will do what I can to keep up with it even when I am not here.

Mr. UPTON. I appreciate that. I just hope that you call a recorded vote because I want to be on record in support of your bill.

Mr. Burr?

Mr. BURR. Thank you, Mr. Chairman. And I will be brief.

I welcome our witnesses today and also pledge to the committee that Mr. Cox is right. We have a responsibility to follow up and to make sure that the efforts by the Department of Energy are in fact fulfilled. And for that reason, Mr. Chairman, I hope that this committee—subcommittee, full committee—will make an inspection of all the facilities after the first of the year; and if in fact the subcommittee or the full committee won't, I will promise our witnesses, I will.

I yield back.

Mr. UPTON. Dr. Ganske, would you care to make a public opening statement?

Mr. GANSKE. Thank you, Mr. Chairman for holding the hearing, and I look forward to the testimony.

Mr. UPTON. Okay. We had alerted members of the Energy and Power Subcommittee that they would be welcome to sit in on the committee and ask questions, and with that in mind, I will recognize Mrs. Wilson for an opening statement.

Mrs. WILSON. Thank you, Mr. Chairman. I appreciate your willingness to allow me to sit in on your subcommittee today. As you know, it is something of particular interest to me, both because of the district that I represent and because of my service on the Select Committee on Intelligence. I will be very interested to hear from the witnesses about a number of things.

As all of you in the room know, there is a significant increase in funding for cyber security in this year's budget. I am interested to see what the plans are for meeting that emerging threat even in open, or in closed session, and how you are planning to implement change. There are a number of new authorities that are given to the Department of Energy in the Defense authorization bill and the Intelligence authorization bill this year with respect to security and safeguards. And what are your plans and where are we going from here?

I am very interested to hear from the witnesses about that, and that also relates to the establishment of a new nuclear security agency, which came about precisely because of some of the problems that we are trying to oversee and investigate here. What is the plan for the transition to that new nuclear security agency and

how are you going to integrate the need for continuing vigilance in safeguards and security in that transition?

And I appreciate the willingness and the openness of the Chair to allow me to participate. Thank you.

Mr. UPTON. Thank you.

We welcome as our first panel Mr. Glenn Podonsky, Director of the Office of Independent Oversight and Performance Assurance at the Department of Energy; General Eugene Habiger, Director of the Office of Security and Emergency Operations, also of the Department of Energy; Mr. Ed Curran, Director of the Office of Counterintelligence, Department of Energy.

As two of you have testified before, you know that it is a long-standing tradition of this subcommittee to take testimony under oath. Do you have any objection to that?

Mr. CURRAN. No, sir.

Mr. PODONSKY. No, sir.

Mr. HABIGER. No, sir.

Mr. UPTON. We also allow under House rules and committee rules you to have counsel available if you desire to have such. Do you need or desire to have counsel?

Mr. CURRAN. No, sir.

Mr. UPTON. Stand and raise your right hands.

[Witnesses sworn.]

Mr. UPTON. You are now under oath.

We actually have a new clock. The egg timer is going to the Smithsonian. We will see if this really does work. Your entire testimony is certainly made a part of the record, and I will start this over again. If you would limit your remarks to 5 minutes, that would be terrific.

TESTIMONY OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE; EUGENE E. HABIGER, DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS; AND EDWARD J. CURRAN, DIRECTOR, OFFICE OF COUNTERINTELLIGENCE, U.S. DEPARTMENT OF ENERGY

Mr. PODONSKY. Thank you, Mr. Chairman. I appreciate the opportunity to once again appear before this committee to discuss our independent oversight activities at the DOE national weapons laboratories. As you stated, I am the Director of the Office of Independent Oversight and Performance Assurance, which 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.

My testimony will include an update on our follow-up efforts at Lawrence Livermore National Laboratory as well as a summary of our recent inspections at Los Alamos and Sandia National Laboratories.

Let me first cover Lawrence Livermore National Laboratory. As you may recall, we provided classified briefings to the members of this committee on July 1 and July 20 of this year on the results of our May inspection of safeguards and security programs at the Lawrence Livermore National Lab. To summarize the results, we

noted several positive attributes at the laboratory, including security upgrades in the Superblock, which is the building complex at Livermore where special nuclear material is used and stored.

We also noted effective implementation of many of the aspects of the Secretary's upgrades and initiatives in the area of computer security, which is now referred to as "cyber security" and which encompasses the measures designed to protect information on DOE computer systems from unauthorized access from hackers who might try and penetrate the computer networks over the Internet, and from system users who could try and exploit vulnerabilities to gain access to information for which they are not authorized.

However, there were weaknesses in protection of classified weapons parts. These are nonnuclear components of the nuclear weapons access controls at areas where classified weapons information was used and stored, and unclassified cyber security which refers to the cyber security measures designed to protect sensitive, but unclassified, information such as unclassified research data and medical records and the like.

Also, Livermore had not done sufficient performance testing to demonstrate that the protective force could reliably perform its mission.

We have scheduled a formal follow-up review at Livermore's site in December of this year. This review will include onsite reviews of Livermore safeguards and security programs as well as extensive scanning of the networks and penetration testing using techniques that hackers would use. The review will also include a detailed assessment of progress on the Livermore corrective action plan, including actions taken by headquarters and the Oakland operations office to support and verify the provisions of the Livermore corrective action plan.

Although the formal review has not yet taken place, we have been closely monitoring the progress on the corrective action plan and have provided comments on several occasions. In general, we are satisfied that our findings are being addressed and that compensatory security measures have been put in place to provide additional security until final resolution of the identified issues.

As part of our ongoing follow-up efforts we have been particularly focusing on Livermore vulnerability assessments and performance testing of the protective force's ability to respond effectively to defeat a terrorist attack at the Superblock. We recognize that Livermore faces some difficult situations as they try to improve their performance testing program while still ensuring that tests are conducted with the highest regard for safety. On several occasions, we have sent some of our inspectors out to Livermore to observe their planning efforts and performance tests and to provide constructive independent oversight input.

Overall, we believe that Livermore has made improvements in their security posture in the Superblock, and the performance testing efforts are more rigorous and realistic. While much work remains to be accomplished, Livermore has demonstrated a rigorous approach to identifying and correcting weaknesses. If Livermore fully implements their current plans for upgrading their security posture and maintains the current attitude of continuous improvement, there is good reason to be optimistic that Livermore and the

safeguards and security program will be improved by the time of our follow-up inspection.

At Sandia National Laboratories in New Mexico we found effective programs in the areas of material control and accountability, protective force and physical security systems. Sandia has taken several actions to upgrade security, such as repositioning protective force members to provide tactical response, procuring armored vehicles with enhanced capabilities, adding barriers to protect the protective force members at the material access area entrance, and improving protective force training. While some weaknesses were identified in the vulnerability assessment and performance test arena, Sandia corrected the most significant issues promptly while we were there.

Sandia also has generally adequate programs in the classified cyber security arena where they are further making improvements. Senior Sandia managers demonstrated their commitment to completing the enhancements identified in the Trilab nine-point plan—

Your egg beater went off.

Mr. UPTON. I see that it did. I was wondering if it was going to ding. But you may continue.

Mr. PODONSKY. [continuing] they identified in their Trilab nine-point plan by allocating resources to achieve its provisions. Although programmatic strengths were noted at Sandia, there were weaknesses again in the unclassified cyber security, protection of classified parts, access controls in areas where classified matter is used and stored, and control of foreign visitors and assignees. For example, Sandia needs to strengthen the fire wall that protects the sensitive unclassified network from the open network and the Internet.

Because of these weaknesses, Sandia received an overall marginal rating. A marginal rating is the middle rating in our three-tier rating system. The highest rating is satisfactory and the lowest is unsatisfactory. A marginal rating indicates that prompt attention and timely improvement is needed, but does not imply that special nuclear material or classified and sensitive information are at immediate risk.

Sandia has submitted corrective action plans, as required, and independent oversight has provided comments to ensure that the issues are fully addressed. We plan a formal follow-up here, too, in December that will assess the progress and the status of the program. As with all of our follow-ups, we will review the status of the identified weak programs, perform extensive cyber security testing and review the corrective action plan.

We performed our inspection at Los Alamos National Laboratory in August. Los Alamos earned an overall satisfactory rating. They have effectively addressed long-standing problems in the accountability of nuclear materials and made significant progress in addressing deficiencies in the protection of classified weapons parts. Los Alamos made additional improvements in the protection of classified weapons parts actually during our inspection. Los Alamos had also added protective force personnel and implemented a rigorous program to control the use of desktop computer modems.

Classified cyber security programs were found to be adequate, and Los Alamos is making progress also on the Trilab nine-point plan.

Additionally, Los Alamos has significantly reduced risks associated with weaknesses in unclassified cyber security systems by installing an effective fire wall configuration to prevent hackers from gaining access to sensitive networks.

The most significant residual weakness was the ability of the unclassified cyber security program to protect against the insider threat. A particular concern related to foreign nationals that were permitted on the unclassified network which had numerous potentially exploitable weaknesses. During the inspection, Los Alamos developed and began implementing an effective plan to address the residual weaknesses, both short-term and long-term. Although significant progress has been made, there is still work to be done in order to achieve the goal of fully satisfactory programs at all DOE sites.

At the three national laboratories only Los Alamos receives and earns an overall satisfactory rating; the other laboratories were rated marginal. However, based on their corrective action plans, we believe that Livermore and Sandia are on the right track to make improvements needed to achieve the satisfactory rating. Although Los Alamos earned an overall satisfactory as with the other sites we plan to perform follow-up activities and continue to monitor their progress.

If I might, Mr. Chairman, in looking at the weaknesses in DOE safeguards and security for the last 15 years, it is important to keep a sense of perspective. In general, protection of our most critical assets such as nuclear weapons components and special nuclear material has improved significantly since the 1980's. While problems are still evident, they are generally degradations in one layer of a multilayered security system rather than the gaping holes of the type frequently noted in the 1980's.

In addition, inspections indicate that sites are complying with the requirements for protecting classified documents, and classified computer systems are generally well protected from hackers. While the gaping holes have not reappeared, attention to security was very much in decline during the mid-90's, and some sites did not adequately analyze the impact of the cuts in security personnel or security measures before implementing those cuts.

In our reviews of the national laboratories, it is very clear that laboratory management has heard the wakeup call from the Secretary and from the Congress. Safeguards and security is receiving a high level of attention from senior management, and we are seeing some improvements that could not have been made without management support and without Secretary Richardson's direct involvement. For example, the establishment of an effective fire wall and the consolidation of classified parts at Los Alamos were actions that we had previously experienced resistance by Los Alamos line managers because of the operational inconvenience. The need for these actions had been identified on previous inspection reviews, but were not implemented because safeguards and security was given relatively low priority.

In the past year, however, we can report that senior management has increased emphasis on safeguards and security and many

important enhancements have been implemented in a way that provides a better balance between safeguards and security and requirements and operational needs. One of the key elements of the recent progress that we have seen is accountability. Secretary Richardson has sent the message that senior DOE and contract managers are accountable for safeguards and security. The Secretary has stated that, "People are getting the message" and that "we're serious about protecting our national secrets." The results of our recent inspections demonstrate that the message has been heard and that actions are being taken at all of our locations that we have inspected.

In conclusion, it is clear that a positive trend has been established, but that a tremendous amount of work still remains to be accomplished. We will not be satisfied as an oversight body until all DOE sites achieve and maintain a fully satisfactory program. However, it is encouraging to note that safeguards and security programs at all three national weapons laboratories have received high levels of management attention over the past year, and there have been significant improvements.

Thank you, Mr. Chairman.

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

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

Thank you Mr. Chairman. I appreciate the opportunity to once again appear before this committee to discuss our Independent Oversight activities at the DOE national weapons laboratories. I am the Director of the Office of Independent Oversight and Performance Assurance, which 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.

This discussion will include an update on our follow-up efforts at the Lawrence Livermore National Laboratory, as well as a summary of the results of our recent inspections at the Los Alamos National Laboratory and Sandia National Laboratories.

Let me first cover the **Lawrence Livermore National Laboratory**. As you may recall, we provided classified briefings to members of this committee on July 1st and July 20th on the results of our May 1999 inspection of safeguards and security programs at the Lawrence Livermore National Laboratory. To summarize the results, we noted several positive attributes at the Lawrence Livermore National Laboratory including security upgrades in the Superblock (the building complex at Livermore where special nuclear material is used and stored). We also noted effective implementation of many aspects of the Secretary's upgrades and initiatives in the area of computer security, which is now referred to as "cyber security" and which encompasses the measures designed to protect information on DOE computer systems from unauthorized access from hackers who might try and penetrate computer networks over the Internet and from system users who could try and exploit vulnerabilities to gain access to information for which they are not authorized. However, there were weaknesses in protection of classified weapons parts (non-nuclear components of nuclear weapons), access controls at areas where classified weapons information was used and stored, and unclassified cyber security (which refers to the cyber security measures designed to protect sensitive but unclassified information, such as unclassified research data and medical records). Also, Livermore had not done sufficient performance testing to demonstrate that the protective force could reliably perform its mission.

We have scheduled a formal follow-up review of the Lawrence Livermore site in December 1999. This review will include onsite reviews of Livermore safeguards and security programs as well as extensive scanning of the networks and penetration testing using techniques that hackers would use. The review will also include a detailed assessment of progress on the Livermore corrective action plan, including actions taken by Headquarters and the Oakland Operations Office to support and verify the provisions of the Livermore corrective action plan. Although the formal

review has not yet taken place, we have been closely monitoring the progress on the corrective action plan and have provided comments on several occasions. In general, we are satisfied that our findings are being addressed and that compensatory security measures have been put in place to provide additional security until final resolution of the identified issues.

As part of our ongoing follow-up efforts, we have been particularly focusing on Livermore vulnerability assessments and performance testing of the protective force's ability to respond effectively to defeat a terrorist attack at the Superblock. We recognize that Livermore faces some difficult situations as they try to improve their performance testing program, while still ensuring that tests are conducted with the highest regard for safety. On several occasions, we have sent some of our specialists to Livermore to observe their planning efforts and performance tests, and to provide constructive Independent Oversight input.

Overall, we believe that Livermore has made improvements in their security posture in the Superblock and the performance testing efforts are more rigorous and realistic. While much work remains to be accomplished, Livermore has demonstrated a rigorous approach to identifying and correcting weaknesses. If Livermore fully implements their current plans for upgrading the security posture and maintains the current attitude of continuous improvement, there is good reason to be optimistic that the Livermore safeguards and security program will be much improved by the time of our follow-up review in December.

At **Sandia National Laboratories** in New Mexico, we found effective programs in the areas of material control and accountability, the protective force, and physical security systems. Sandia has taken several actions to upgrade security, such as repositioning protective force members to improve tactical response, procuring armored vehicles with enhanced capabilities, adding barriers to protect the protective force members at the "material access area" entrance, and improving protective force training. While some weaknesses were identified in the vulnerability assessment and performance test arena, Sandia corrected the most significant issue promptly by adding the barriers at the material access area.

Sandia also had generally adequate programs in the *classified* cyber security arena and were making further improvements. Senior Sandia managers demonstrated their commitment to completing the enhancements identified in the "Tri-Lab nine point plan" by allocating resources to achieve its provisions.

Although programmatic strengths were noted at Sandia, there were weaknesses in *unclassified* cyber security, protection of classified parts, access controls in areas where classified matter is used and stored, and control of foreign visitors and assignees. For example, Sandia needs to strengthen the firewall that protects the sensitive unclassified network from the open network and the Internet. Because of these weaknesses, Sandia received an overall "Marginal" rating. A Marginal rating is the middle rating in OA's three tier rating system, the highest rating is Satisfactory and the lowest is Unsatisfactory. A Marginal rating indicates that prompt attention and timely improvement is needed but does not imply that special nuclear material or classified and sensitive information are at immediate risk.

Sandia has submitted their corrective action plans as required and Independent Oversight has provided comments to ensure that the issues are fully addressed. We plan a formal follow-up review in December that will assess the progress and status of the program. As with all of our follow-up reviews, we will review the status of all identified weak programs, perform extensive cyber security testing, and review the corrective action plan provisions.

We performed our inspection of the **Los Alamos National Laboratory** in August of 1999. Los Alamos earned an overall "Satisfactory" rating. Los Alamos had effectively addressed long-standing problems in the accountability of nuclear materials, and made significant progress in addressing deficiencies in the protection of classified weapons parts. Los Alamos made additional improvements in the protection of classified weapons parts during the inspection. Los Alamos had also added protective force personnel and implemented a rigorous program to control the use of desk top computer modems. Classified cyber security programs were found to be adequate, and Los Alamos is making progress on the "Tri-Lab nine-point" plan. Additionally, Los Alamos has significantly reduced risks associated with weaknesses in unclassified cyber security systems by installing an effective firewall configuration to prevent hackers from gaining access to sensitive networks.

The most significant residual weakness was in the ability of the unclassified cyber security program to protect against the insider threat. A particular concern related to foreign nationals that were permitted on the unclassified network, which had numerous potentially exploitable weaknesses. During the inspection, Los Alamos developed and began implementing an effective plan to address the residual weaknesses both in the short term and long term.

Although significant progress has been made, there is still work to be done in order to achieve the goal of fully satisfactory programs at all DOE sites. At the three national weapons laboratories, only the Los Alamos National Laboratory was assigned an overall Satisfactory rating. The other two laboratories were rated Marginal. However, based on their corrective action plans, we believe that Livermore and Sandia are on track to make improvements needed to achieve a Satisfactory rating. Although Los Alamos earned an overall "Satisfactory" rating, as with the other sites, we plan to perform follow-up activities and continue to monitor their progress in implementing their corrective action plan.

In looking at the weaknesses in DOE safeguards and security programs, it is important to keep a sense of perspective. In general, protection of our most critical assets, such as nuclear weapons components and special nuclear materials, has improved significantly since the 1980s. While problems are still evident, they are generally degradations in one layer of a multi-layered security system rather than gaping holes of the type frequently noted in the 1980s. In addition, inspections indicate that sites are complying with requirements for protecting *classified* documents, and classified computer systems are generally well protected from hackers. While the gaping holes have not reappeared, attention to security was in decline during the mid-1990s and some sites did not adequately analyze the impact of cuts in security personnel or security measures before implementing those cuts.

In our reviews of the national weapons laboratories, it is very clear that laboratory management has heard the wake up call from the Secretary. Safeguards and security is receiving a high level of attention from senior management and we are seeing some improvements that could not have been made without management support and Secretary Richardson's involvement. For example, the establishment of an effective firewall and the consolidation of classified parts at Los Alamos were actions that had previously been resisted by the Los Alamos line managers because of the operational inconvenience. The need for these actions had been identified on previous Independent Oversight reviews but were not implemented because safeguards and security was given relatively low priority. In the past year, however, senior management has increased emphasis on safeguards and security and many important enhancements have been implemented in a way that provides a better balance between safeguards and security requirements and operational needs.

One of the key elements of the recent progress is increased accountability. Secretary Richardson has sent the message that senior DOE and contractor managers are accountable for safeguards and security. This has been accomplished through various measures; a few examples include:

- The reorganization of responsibilities at DOE Headquarters, which established the Lead Program Secretarial Office as responsible and accountable for safeguards and security
- The "zero tolerance policy" which establishes expectations for safeguards and security and accountability at all levels of line management from the first level supervisor to the laboratory directors and to DOE operations office managers and DOE program offices

The Secretary has stated [quote] "People are getting the message that we're serious about protecting our nation's secrets" [unquote]. The results of our recent inspections demonstrate that the message has been heard and that actions are being taken to improve the safeguards and security posture at our national laboratories.

In conclusion, it is clear that a positive trend has been established but that much work remains to be accomplished. We will not be satisfied until all DOE sites achieve and maintain a fully satisfactory program and establish processes for ensuring continuous improvement. However, it is encouraging to note that safeguards and security programs at all three national weapons laboratories have received high levels of management attention over the past year and there have been significant improvements.

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

Mr. UPTON. General Habiger.

TESTIMONY OF EUGENE E. HABIGER

Mr. HABIGER. Mr. Chairman, it is my first opportunity to testify before this committee.

Mr. UPTON. All of these butterflies flying all around.

Mr. HABIGER. As most of you are aware, Secretary Richardson asked me to become the Department Security Director in June. Since my arrival, I have visited all the Department's major sites,

reviewed virtually all of our site protection plans, observed and participated in segments of our protective force training at our central training facility, examined our newly implemented cyber security procedures at our national laboratories, talked to hundreds of scientists and technicians and taken a DOE-administered polygraph. What I have found so far is this:

First, it is clearly obvious that the Department reacted appropriately to the wakeup call received this past year with the uncovering of internal security problems and the publication of both the Cox and the Rudman reports.

Second, security throughout the Department is being administered responsibly and conscientiously by dedicated hard-working professionals who are firmly committed to protecting the national security assets which are entrusted to them.

Finally, although we do have security issues which we must and will address, I found all sites that I have visited have the foundation to perform their security functions capably, given adequate resources.

But I also discovered some troubling issues. First and foremost, it was apparent to me early on that the Department was extremely close to losing the confidence and special trust of both the American people and the Congress with respect to our ability to perform our security responsibilities.

Second, and equally as important, I discovered that over the years the Department had lost its focus on security; and you said it best in your opening remarks, sir, that we had a dysfunctional organization. There was no office within the Department that had ultimate accountability for the security requirements for which DOE is responsible, nor was there any emphasis on individual accountability. By-products of this organizational dysfunction and lack of focus included a deterioration of security awareness and education, resulting in a failure to remind and educate our employees and contractors as to their personal security responsibilities and accountabilities.

Finally, Congress, up to this point, has failed to fund the Department's fiscal year 2000 full budget amendment in order to make near- and long-term fixes. We have, Mr. Chairman, valid requirements in the area of cyber security to buy hardware encryption equipment and to train our systems administrators. We need to equip our protective forces with equipment to combat weapons of mass destruction, and we need program direction funds to stand up a viable foreign visitor access program, as well as an acceptable plutonium, uranium, and special nuclear materials control and accountability program.

Simply stated, we have been given a mandate, but not the resources to accomplish that mandate. Though a series of comprehensive and sweeping initiatives by Secretary Richardson, the Department has, however, turned the corner, in my view, and has aggressively and dynamically changed the way it does its security business.

Soon after coming on board, I put into motion an aggressive four-phased security campaign. In Phase I, which was completed in August, I initiated visits to all major DOE sites. We established a

baseline from which to move forward. We found a number of things that needed to be fixed quickly, and we did that very, very quickly.

Phase II, currently under way, I completed visits to the sites and issued or am in the process of issuing policy addressing key issues such as standardization of weapons for our protective forces, the requirement for our protective forces to keep a round in the chamber of their weapons while on duty. We weren't training the way we would fight. We now have policies which we never had before, which mandate the timely reporting of security incidents, the use of warning banners on computer systems and badge validation procedures.

In the area of cyber security, the national laboratories have implemented numerous corrective actions. Key among them is a program to achieve physical incompatibility between removable media formats within common laboratory work areas.

In Phase III, which will occur in January through March of next year, most of the new policies to fix security problems will have been implemented and I will revisit the field to establish the effectiveness of those policies.

When we reach Phase IV in April to September of next year, proposed fixes will be in place and our efforts turned toward minor adjustments as we maintain our security program.

Today, the Department of Energy is in a security environment decidedly different from the one we faced a decade earlier. There is a growing concern about a new breed of threats that confront the Department and the Nation's security structures. Terrorism, weapons of mass destruction and cyber attacks on information systems have become ingrained in the global psyche and our Nation's security consciousness. This is a significant challenge, Mr. Chairman, but one that the Department of Energy is prepared to meet.

[The prepared statement of Eugene E. Habiger follows:]

PREPARED STATEMENT OF EUGENE E. HABIGER, GENERAL, USAF (RETIRED), DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS, U.S. DEPARTMENT OF ENERGY

I would like to thank the Chairman and Members of the Committee for the opportunity to speak with you today regarding the current status of security at the Department of Energy.

As most of you are aware, Secretary Richardson asked me to become the Department's Security director in June. Since my arrival at the Department, I have visited all of the Department's major sites...Reviewed virtually all of our site security plans...Observed and participated in segments of our protective force training at our training facility in Albuquerque, New Mexico...Examined our newly implemented cyber security procedures at our national laboratories...Talked to hundreds of scientists and technicians...And, taken a DOE-administered polygraph.

What I have found so far is this:

First, it is clearly obvious that the Department reacted appropriately to the "wake up call" received this past year with the uncovering of internal security problems and the publication of both the Cox and Rudman reports.

Second, security throughout the Department is being administered responsibly and conscientiously by dedicated, hard working professionals who are firmly committed to protecting the critical national security assets which are entrusted to them. The responsibilities of these individuals are demanding—yet, despite the obvious challenges, they continue to perform in an outstanding manner.

Finally, although we do have security issues which we must, and will, address, I found all sites that I have visited have the foundation to perform their security functions capably given adequate resources.

But I also discovered several troubling issues.

First and foremost, it was apparent to me early on that the Department was extremely close to losing the confidence and trust of both the American people and the Congress with respect to our ability to perform our security responsibilities. The enormous media coverage surrounding recent security related events coupled with DOE's historical track-record of security deficiencies added to this erosion of public trust.

Secondly and equally as important, I discovered that over the years the Department had lost its focus on security. The Secretary on several occasions has referred to the Department as being a group of fiefdoms within fiefdoms—and almost every fiefdom had its own security responsibility and security budget. There was no office within the Department who had ultimate accountability for the critical security requirements for which DOE is responsible nor was there any emphasis on individual accountability. By-products of this organizational dysfunction and lack of focus included: a deterioration of security awareness and education resulting in a failure to remind and educate our employees and contractors as to their personal security responsibilities and accountabilities...lack of attention to our cyber security practices in a world of increased computer hacking and cyber terrorism...And, a gradual erosion of resources required to improve our capabilities to combat ever-changing terrorist and cyber-terrorist threats.

And finally, Congress has, up to this point, failed to fund the Department's FY2000 full budget amendment in order to make near and long-term fixes. We have valid requirements in the area of cyber-security to buy hardware, encryption equipment and to train our system administrators. We need to equip our protective forces to combat weapons of mass destruction...to fully arm the headquarters protective forces and complete our headquarters security upgrades...And, we need program direction funds to stand up a robust foreign visitor access program as well as an acceptable plutonium, uranium and special nuclear materials control and accountability program and bring about our new organization. Simply stated, we have been given a mandate but not the additional resources to accomplish that mandate.

Through a series of comprehensive and sweeping initiatives by Secretary Richardson, however, the Department has turned the corner and has aggressively and dynamically changed the way it does its security business.

In May of this year Secretary Richardson announced his Security Reform Package—the most sweeping reform of security programs in the Department's history. This comprehensive plan involved the creation of my office—the Office of Security and Emergency Operations, and the elevation and revitalization of Mr. Glenn Podonsky's Office of Independent Oversight and Performance Assurance. In the words of Secretary Richardson, "this plan gives DOE the tools and authority we need to *detect* security infractions, *correct* institutional problems and *protect* America's nuclear secrets." Glenn and I are working closely together to ensure an integrated approach to policy development and oversight.

The foundation of the Secretary's security reform plan is his policy statement regarding security incidents and violations. In his statement, the Secretary established an expectation of personal accountability by DOE employees and contractors for protecting DOE's national security assets. The Secretary further established a policy of zero tolerance for violations of security requirements that could place nuclear or other sensitive information at risk.

Another important step was to change the way the Department managed its security responsibilities. In this regard, the Secretary worked diligently to remove the organizational barriers that had historically impeded the Department's ability to effectively and efficiently implement a comprehensive security program within the Department.

Soon after coming on board I put in motion an aggressive, Four-Phased Security Campaign. In Phase I, which was completed in August, I initiated visits to each of the DOE sites in the field, and established a baseline from which to move forward. Areas requiring immediate fixes were identified. During this period, a complex-wide security stand-down was conducted to promote security awareness as an individual responsibility. New policy was issued for foreign visitors who visit our facilities to ensure that the tightest possible security procedures are followed.

In Phase II, currently underway, I completed visits to the sites and issued, or am in the process of issuing, policy addressing key issues, such as: Standardized Weapons for Protective Forces, and the requirement for protective forces to keep a round in the chamber of weapons carried while on duty. We now have policies which mandate the timely reporting of security incidents, the use of warning banners on computer systems, and badge validation procedures. We are developing an integrated security awareness training curriculum. Two very similar personal security assurance programs will be combined into a single departmental Human Reliability Program to eliminate redundancy and streamline the administration process. In the

area of cyber-security, the National Laboratories have implemented numerous corrective actions. Key among these is a program to achieve physical incompatibility between removable media formats within common laboratory work areas. We are taking this sweeping action in an effort to prevent the intentional or inadvertent transfer of classified information from classified to unclassified systems or to a media format easily concealed and removed. In related efforts, the laboratories will continue to search unclassified archives and to monitor outgoing e-mail messages for classified content. We are also developing a comprehensive set of metrics to make sure we are making continuous improvements.

Phase III will occur in January to March of 2000, at which time most new policies to fix security will have been implemented. I will revisit the field to evaluate the effectiveness of the policies and to define metrics to be used for future assessments. At this stage, most of the major security concerns will be fixed and the focus turned to improvements and enhancements.

When we reach Phase IV in April to September of 2000, proposed fixes will be in place and our efforts turned toward adjustments, as we maintain our security program. A critical activity here will be continuous feedback from the field, scheduled visits to the field, and regularly held meetings with representatives from all sites to exchange lessons learned and best practices.

Successful implementation of our security responsibilities will also depend on a focused and well-defined mission and management structure that addresses policy and decision making, personnel and budget resources, planning and program execution. Therefore, we are *reconstituting available resources into a robust, responsive, and unified safeguards and security organization*. This was the Secretary's intent when he announced his security reform initiative; and we are making real progress.

Our workforce—both Federal and contractor—is the most critical link in the chain of protection of security interests. Consequently, we are instilling a sense of urgency and corporate ownership among all Department of Energy employees and contractors, not just those that have security as part of their job descriptions. This is being accomplished through renewed emphasis on a meaningful enforcement program that holds individuals accountable should they violate their security responsibilities.

We are enhancing our efforts to ensure that employees are fully aware of their own individual protection responsibilities. The granting of a security clearance carries with it a very serious obligation to protect the sensitive and critical assets entrusted to one's care. We have mounted an aggressive and comprehensive security education and awareness campaign to remind each and every individual of their obligations.

For those individuals whose primary duties relate to the protection of national security assets (that is, our security professionals), we are instituting a comprehensive career development initiative that establishes a centrally managed competency based promotion and assignments program designed to institute staffing uniformity and enhanced operability throughout the complex. This program is an adaptation of existing programs in place with other government agencies, the military and private industry. It represents what I believe to be a "best practice" in the area of career development.

Finally, recognizing our critical role in the national security community, we are institutionalizing my office as the principal security coordinator for the Department in developing inter- and intra-agency partnerships. In so doing we actively contribute to the protection of the Nation's energy infrastructure and leverage technology and, as applicable, expertise into the international security community dealing with nuclear safeguards and security.

Today, the Department of Energy functions in a security environment decidedly different from the one we faced a decade earlier. There is growing concern about a new breed of threats that confront the Department and the Nation's security structures. Terrorism, Weapons of Mass Destruction and cyber attacks on information systems have become ingrained in the global psyche and in our nation's security consciousness. These non-traditional, multi-directional threats are testing security resolve and capabilities as never before.

We cannot control or alter the threats to the security interests entrusted to our care. What can be controlled, however, is our ability to plan and respond to threats should they ever materialize. The changing security environment and other threats over the past decade have fundamentally altered the Department's security perspective and posture. This is a significant challenge, but one that the Department of Energy is prepared to meet.

Mr. UPTON. Thank you. Pretty close on the time as well.
Mr. Curran.

TESTIMONY OF EDWARD J. CURRAN

Mr. CURRAN. Good morning. Mr. Chairman, I am happy to be here this morning to discuss the state of counterintelligence at the Department of Energy. As you are aware, I have been the Director of the Office of Counterintelligence at DOE since April 1, 1998. In the 1½ years since I have assumed this position, I believe DOE has made significant progress toward developing an effective and efficient program to protect DOE personnel and facilities, as well as classified and sensitive unclassified information on foreign intelligence threats. This progress would not have been possible without the strong support of Secretary Bill Richardson and the Congress.

Before I discuss the specific progress that has been made to date, I would like to provide some background on the counterintelligence at DOE.

PDD-61, captioned U.S. Department of Energy Counterintelligence Program, was signed by President Clinton on February 11, 1998. The PDD was the result of numerous General Accounting Office reviews, United States intelligence community assessments, and a Federal Bureau of Investigation study directed by the Senate Select Committee on Intelligence in April 1997. The PDD required that I prepare a report for the Secretary of Energy 90 days after my arrival to include an assessment of the current state of DOE's CI program, a strategic plan for achieving long-term goals and objectives of the PDD, and an action plan for near-term measures to reduce the foreign intelligence threat to DOE laboratories.

To accomplish this effort, I pulled together a team of CI experts, security professionals, and individuals with cyber expertise from throughout the Intelligence Community. The resulting report, captioned Mapping the Future of the Department of Energy's Counterintelligence Program, hereinafter referred to as the 90-Day Study, identified many deficiencies in DOE's CI program and further verified that the program didn't meet minimal standards.

The review was initiated on April 1, 1998, and concluded on July 1, 1998, when the 90-Day Study was submitted to the Secretary of Energy, the Secretary of Defense, the Attorney General, the Director of Central Intelligence and the Director of the FBI. The report made 46 concrete recommendations to improve the effectiveness and efficiency of the DOE CI program.

On November 13, 1998, Secretary Richardson approved virtually all of the 46 recommendations identified in the 90-Day Study and furnished DOE's CI action plan to Mr. Sandy Berger, Assistant to the President for National Security Affairs. In the Secretary's CI action plan, my office was directed to prepare a CI implementation plan within 45 days of the issuance of the action plan. This OCI implementation plan was delivered to the Office of Secretary on February 3, 1999. In the implementation plan, we assigned individual offices primary and supporting responsibility for each recommendation. We have since prioritized the 46 recommendations into three different tiers.

I would like to assure you that even while my office was preparing the CI implementation plan we were also in the process of implementing many of the 90-Day Study's recommendations. I am pleased to inform you that, to date, approximately 75 percent of the 46 recommendations have been implemented. Furthermore, almost

95 percent of the 24 Tier I recommendations have been implemented.

I would like to take a few minutes to identify some of these implementation successes and elaborate on many of the procedures we have already put into place to address the deficiencies in DOE's CI program.

The most important part of developing a world-class CI program is, of course, the resources. Historically, the DOE CI program has been underfunded and skills mix of the employees has been insufficient to effectively execute a complex-wide CI mission. Currently, the Department has over 110,000 cleared individuals placed in 50 laboratories and facilities, most of which are under separate contracts. These laboratories and facilities house most of the Nation's premier scientists' research and development and the most sophisticated technology applications in the world. Yet when I came on board in April, 1998 to head the Department's CI efforts, DOE had only seven full-time Federal employees at the headquarters dedicated to the CI mission and just a few untrained CI officers in the field. Seven of these CI officers reported to their separate laboratories or facility management without any consolidated headquarters oversight or direction for their programs.

Today, I have a staff of 130 Federal, contractor, and Intelligence Community CI professionals. I expect this number to increase to 156 by the end of this fiscal year. Next fiscal year, it is our goal to hire a significant amount of CI-cyber experts and place them at select DOE facilities. Importantly, at each of the five weapons laboratories, I have hired with the cooperation of all the lab directors seasoned CI professionals, all of whom are retired FBI special agents. These CI officers are no longer buried in the local bureaucracy. They have direct access to me and to the laboratory director should they need to discuss a CI matter.

The DOE CI program began in 1988, and from its inception through 1996 the Department spent less than \$3 million annually on counterintelligence. In fiscal years 1997 and 1998, the Intelligence Committees approved a supplement for DOE's CI budget based on numerous GAO reports and their continued significant concerns regarding visitors at the laboratories. This supplement brought the total CI program funding to \$6.6 million in 1997, and \$7.6 million in the 1998. Since my appointment in April of last year, I have successfully increased DOE's CI budget from \$7.6 million to \$15.6 for fiscal year 1999, and \$39.2 million, which includes \$8 million for CI cyber initiatives, for this fiscal year.

This very tedious and exhaustive effort was accomplished with exceptional support from Secretary Richardson and members of the House Armed Services Committee and the House and Senate Select Committees on Intelligence. Without their continued support and push for adequate financing, none of the improvements to DOE's CI program, which I am about to describe, would have been possible.

Direct funding, along with headquarter's OCI control and direction of funds to the laboratories and other DOE facilities is the cornerstone of the 90-Day Study, the CI action plan and the CI implementation plan and an overall effective CI program at DOE. Without this level of control, meaningful oversight is impossible. Direct

funding has helped us to have great control over allocation of resources to the priorities I have set for the CI program. I would like to share with you these programmatic priorities and the efforts OCI is undertaking to improve the DOE CI program.

First, I will highlight some of the very critical and necessary changes in day-to-day operations of the CI effort at DOE headquarters. As a result of PDD-61, a new independent Office of Counterintelligence was created that reports directly to the Secretary of Energy. As Director of OCI, the PDD gives me direct CI policy development, implementation and oversight responsibilities for all CI activities throughout DOE. The Secretary signed a delegation order confirming those responsibilities and delegating to me the appropriate authority to execute them. In addition to my direct reporting and access to the Secretary on CI issues, on a regular biweekly basis, I meet with Under Secretary Moniz and Deputy Secretary Glauthier on CI issues or as need arises. Mr. Sanchez from the Office of Intelligence and I both participate in these meetings since our offices work very, very closely together.

As a result of the 90-Day Study findings, I determined that the optimal OCI organizational structure includes six distinct areas: analysis, investigations, CI-cyber training, inspections, and a CI evaluation board. Importantly, each of these programs must operate as a single, integrated program. None of them, taken in isolation, would constitute a viable CI program.

The analysis program is headed by an experienced analyst detailed from the FBI with over 8 years of specific analytical experience. Her deputy is a detailee from the FBI with analytical experience. They both are very familiar with DOE, since they participated in the FBI study of DOE directed by the Senate Select Committee, which I previously mentioned. They have six analysts currently working for them and are in the process of hiring several more experienced analysts. We expect to place CI analysts at five laboratories this fiscal year.

In my opinion, DOE has a wealth of information which has not been analytically exploited in the past. The reports we have produced and will be producing are obviously of great importance to DOE, but also to the Intelligence Community.

For example, a DOE CI analyst played an extremely important role in the preparation of the first annual threat assessment prepared by the National Counterintelligence Center at the direction of the DCI, published in November of last year. This report is required on an annual basis as a result of PDD-61.

OCI analysts are currently playing a critical role in the second annual PDD-61-mandated threat assessment which should be published next month. These reports are a direct result of the President's direction and represent meaningful impact to DOE that I have not seen in the past. In my opinion, if it were not for the tenacious efforts by my DOE analysts in this annual effort, the reports would have been far less meaningful than they are.

The analysis program has written and will continue to write foreign intelligence threat assessments resulting from DOE's extensive interaction with DOE-sensitive countries. As the U.S. Government's technical advisor to various bilateral and multilateral non-proliferation and arms control initiatives, DOE hosts hundreds of

sensitive country foreign nationals each year, and DOE officials are frequent travelers to sensitive countries.

The analysis program is also in the midst of a study of potential economic espionage at the laboratories. The laboratories engage in cooperative research and development agreements, CRADAs, with private industry. OCI wants to ensure that proprietary economic information is being properly protected.

The projects I mentioned above are expensive, but the results and benefits to DOE and the Intelligence Community will allow us to detect and work toward neutralizing foreign intelligence activities directed at DOE. These products also provide our policymakers with the information they need to make national policy decisions.

The investigations program is headed by another FBI supervisor, currently on detail from the FBI, with over 20 years' experience in foreign counterintelligence. His primary responsibility is to ensure that any instances in which classified information is being or may have been compromised to an unauthorized party are reported to the FBI. I will continue to staff this program with qualified and experienced investigators.

The CI cyber program is headed by an employee from the FBI's National Infrastructure Protection Center. The CI cyber program director serves as OCI's representative to DOE's critical infrastructure protection task force. Her daily activities include interaction with DOE headquarters and laboratory computer professionals, as well as the NIPC. With the additional \$8 million OCI received for cyber programs in fiscal year 2000, we are implementing some of the recommendations in the 90-Day Study.

One of the 90-Day Study's recommendations was the development and implementation of a complex-wide strategy to address the potential CI implications of e-mail. As mentioned before, the CI program will significantly enhance the number of CI experts this fiscal year in order to further develop field intrusion detection and analysis abilities. CI cyber personnel require skills in both computer security and counterintelligence.

A DOE Federal employee heads our training program. The purpose of the training program is threefold: to formulate an in-house program to train our own CI personnel, to provide professional awareness briefings and debriefings for our scientists traveling to sensitive countries, and to provide awareness briefings for the general DOE population who have an interface with foreigners so that they become sensitive to CI-related issues. Professional training for CI officers has been reoriented to focus on core skills necessary to be an effective CI person.

I would like to provide some examples of our current outreach and awareness training efforts to the DOE population. The OCI currently has CI professionals assigned to DOE highly enriched uranium transparency program. This person is responsible for all related CI issues and team briefings and debriefings. He is accepted and trusted as a total team member and the members are willing to address sensitive CI issues with him. I have established the same relationship with scientists and DOE employees associated with the Materials Protection and Accounting Program, the largest program within DOE dealing with the Russians, the Initiative for Proliferation Prevention, the Nuclear Cities Initiative, and the

China Arms Control Exchange by assigning a CI officer to each team. Assigning a CI officer to all such programs within DOE will help us to achieve our goal of briefing and debriefing all personnel traveling to sensitive countries. Our CI goal is not only to protect technology, but the programs involving DOE personnel.

Inspections: We have established an internal inspection process required by PDD-61. There are two teams available at any given time to complete these inspections. One team is headed by a retired FBI agent who was the former Assistant Director in charge of the Washington field office and was previously the Deputy Director in the FBI's Inspection Division. The second team is headed by a former Special Agent who retired from the FBI as the Special Agent in charge of the Springfield office and was also an inspector in the FBI's Inspection Division. Both of these individuals have over 25 years' experience in the FBI and specifically in the CI arena. The inspection teams are supported by experienced retired FBI and law enforcement officers who are experts in gathering information and resolving complex cases. The teams have been augmented by senior retired personnel security experts from DOE, along with retired laboratory scientists.

As of this date two inspections have taken place: Los Alamos National Laboratory and Lawrence Livermore National Laboratory. A third inspection of Sandia National Laboratories is under way this week. All DOE facilities are subject to CI inspection, and we have scheduled 12 facilities for inspection next calendar year. The results of the first two inspections have been provided to me and Secretary Richardson.

In brief, these results show that significant improvements have been made in the CI programs in these laboratories since PDD-61 was signed. I will provide summaries of these inspections to Congress in the annual report on counterintelligence and security practices at the national laboratories as mandated by the National Defense Authorization Act for fiscal year 2000. Any significant CI relevant events will be provided to you immediately.

The CI Evaluations Board: PDD-61 authorized the use of many tools designed to reduce the threat to classified and sensitive information at DOE and its field activities. The polygraph was specifically cited as being one of the tools which OCI, in coordination with the DOE Office of Security Affairs, may use to enhance the DOE CI program. Research and analysis conducted for the 90-Day Study all indicated that the polygraph was one tool that could be used to enhance the effectiveness of the CI program.

OCI's Counterintelligence Evaluation Board is responsible for implementing the DOE CI polygraph program. A senior OCI officer is leading OCI's CIEB. I must stress that the polygraph program is only one of six elements of the DOE CI program; it cannot be considered in isolation. I do not believe that the polygraph is a CI panacea or an infallible CI tool. However, I do believe that the polygraph serves as a valuable deterrent to individuals who currently have direct or indirect access to classified information and may be contemplating espionage.

I also believe the polygraph serves as a constructive screening device for individuals applying for positions requiring access to classified and/or sensitive unclassified information. The polygraph

can also be used effectively as an exculpatory tool. The purpose of the polygraph program is to protect U.S. national security by attempting to determine if anyone with access has engaged in espionage, sabotage or terrorism or has had unauthorized contact with foreign nationals or disclosed classified information in an unauthorized manner.

I am extremely sensitive to the anxiety that the polygraph program has caused in the Department. I want to stress that we are only going to be administering the polygraph and examinations to a small percentage of DOE employees having access to the most sensitive high-risk national security programs. These programs include Special Access Programs; Sensitive Compartmented Information, SCI; Personnel Security and Assurance Program, and the Personnel Assurance Program known as PAPS. The latter two programs involve DOE employees who are involved in the design of nuclear weapons and those who have direct access to nuclear weapons.

OCI has made every effort to reach out to potentially affected personnel to explain the polygraph. Technical briefings for employees of Sandia, Lawrence Livermore, Los Alamos National Laboratories were held last month. In accordance with the rulemaking process, OCI participated with General Habiger, Director of the Office of Security and Operations in public hearings. The public hearings were held at Lawrence Livermore National Laboratory in September 1999; Sandia National Laboratory on September 16; Los Alamos, September 17; and Washington, DC, here, September 22.

Additionally, as you are aware, I provided a briefing on the polygraph program to this subcommittee on October 4. We also briefed the White House science advisor on the same program.

While DOE has approved a notice on the polygraph program, it only applies to DOE Federal employees. We're currently in the latter stages of an Office of Personnel Management-mandated rulemaking process to develop regulations for applying the program to DOE contractors. DOE contractors constitute the majority of individuals in the aforementioned high-risk national security programs.

As DOE participates in the rulemaking process necessary to apply to the polygraph program to DOE contractors, we have been simultaneously administering the polygraph to DOE Federal employees and volunteering contract employees in OCI and the Office of Environment, Safety and Health. Additionally, some high-level Department officials, including the Secretary, Deputy Secretary and Under Secretary have taken the polygraph. I was the first to volunteer to take the polygraph last year. Overall, approximately 85 personnel have been administered and passed a CI-scope polygraph thus far.

To ensure quality control, the polygraph program is managed by an individual that has been the quality control on polygraphs for DOE since 1991. He is the Director of Quality Control for the American Association of Police Polygraph Examiners and subcommittee chairman of the Quality Control Committee for the American Polygraph Association.

The OCI polygraph program manager also served as the chief instructor at the Federal Polygraph School from 1985 to 1991 and in Government Service Polygraph since 1974.

The current DOE Polygraph Program has four layers of quality control. This is more than any other U.S. Government agency which administers polygraph examinations.

Mr. UPTON. Mr. Curran, I have been very generous with the time.

Mr. CURRAN. I know. I have one more page.

Our decisions about who is granted access to classified information must be made with the sole criteria of protecting U.S. national security. The enhancement of the DOE Polygraph Program is not without precedent, as our efforts are bringing the Department in line with the rest of the intelligence community insofar as access to high risk national security programs are concerned. I believe that the Department's commitment to the overall CI effort is embodied in its support for the Polygraph Program. OCI has received strong support from the Secretary for this initiative, and with his and your continued support we will continue to use the polygraph as an important CI tool.

Thank you, Mr. Chairman, for your patience.

[The prepared statement of Edward J. Curran follows:]

PREPARED STATEMENT OF EDWARD J. CURRAN, DIRECTOR, OFFICE OF
COUNTERINTELLIGENCE, U.S. DEPARTMENT OF ENERGY

Good afternoon Mr. Chairman. I am happy to be here this afternoon to discuss the state of counterintelligence (CI) at the Department of Energy (DOE). As you are aware, I have been the Director of the Office of Counterintelligence (OCI) at DOE since April 1, 1998. In the one and a half years since I assumed this position, I believe DOE has made significant progress toward developing an effective and efficient program to protect DOE personnel and facilities, as well as classified and sensitive unclassified information, from foreign intelligence threats. This progress would not have been possible without the strong support of Energy Secretary Bill Richardson and the Congress. Before I discuss the specific progress that has been made to date, I would like to provide some background on counterintelligence at DOE.

BACKGROUND

Presidential Decision Directive/NSC 61 (PDD-61), *U.S. Department of Energy Counterintelligence Program*, was signed by the President on February 11, 1998. The PDD was the result of numerous General Accounting Office (GAO) reviews, United States Intelligence Community assessments and a Federal Bureau of Investigation (FBI) study directed by the Senate Select Committee on Intelligence (SSCI) in April 1997. The PDD required that I prepare a report for the Secretary of Energy 90 days after my arrival to include an assessment of the current state of DOE's CI Program, a strategic plan for achieving the long-term goals and objectives of the PDD, and an action plan for near-term measures to reduce the foreign intelligence threat to the DOE laboratories. To accomplish this effort, I pulled together a team of CI experts, security professionals, and individuals with cyber expertise from throughout the Intelligence Community. The resulting report, *Mapping the Future of the Department of Energy's Counterintelligence Program*, hereinafter referred to as the 90-Day Study, identified many deficiencies in DOE's CI Program and further verified that the Program did not meet minimal standards. The review was initiated on April 1, 1998 and concluded on July 1, 1998 when the 90 Day Study was submitted to the Secretary of Energy, the Secretary of Defense, Attorney General, Director of Central Intelligence (DCI) and Director, FBI. The report made 46 concrete recommendations to improve the effectiveness and efficiency of the DOE CI Program.

On November 13, 1998, Secretary of Energy Richardson approved virtually all of the 46 recommendations identified in the 90-Day Study and furnished a DOE CI Action Plan to Mr. Sandy Berger, Assistant to the President for National Security Affairs. In the Secretary's CI Action Plan, my Office was directed to prepare a CI Implementation Plan within 45 days of the issuance of the Action Plan. This OCI Implementation Plan was delivered to the Office of the Secretary on February 3, 1999. In the Implementation Plan we assigned individual offices primary and sup-

porting responsibility for each recommendation. We have since prioritized the 46 recommendations into three tiers.

IMPLEMENTATION PLAN PROGRESS

I would like to assure you that even while my Office was preparing the CI Implementation Plan we were also in the process of implementing many of the 90-Day Study's recommendations. I am pleased to inform you that to date, approximately 75% of the 46 recommendations have been implemented. Furthermore, almost 95% of the 24 most critical ("Tier One"), 60% of the Tier Two, and 50% of the Tier Three recommendations have been implemented. I would like to take just a few minutes to identify some of these implementation successes and elaborate on many of the procedures we have already put into place to address the deficiencies in DOE's CI Program.

Resources

The most important part of developing a world-class CI Program is, of course, the resources. Historically, the DOE CI Program has been underfunded and the skills mix of the employees has been insufficient to effectively execute a complex-wide CI mission. Currently, the Department has over 110,000 cleared individuals placed in over 50 laboratories and facilities, most of which are under separate contracts. These laboratories and facilities house most of the nation's premiere scientists, research and development, and most sophisticated technology applications in the world—yet when I came on board in April 1998 to head the Department's CI effort, DOE had only seven full time Federal employees at headquarters dedicated to the CI mission, and just a few untrained CI Officers in the field. Each of these CI Officers reported to their separate laboratory or facility management without any consolidated headquarters oversight or direction for their programs.

Today I have a staff of 130 Federal, contractor, and Intelligence Community CI professionals; I expect this number to increase to 156 by the end of this fiscal year. Next fiscal year it is our goal to hire a significant amount of CI-Cyber experts and place them at select DOE facilities. Importantly, at each of the five weapons laboratories, I have hired seasoned CI professionals, all of whom are retired FBI Special Agents. These CI Officers are no longer buried in the local bureaucracy; they have direct access to me and to the Laboratory Director should they need to discuss a CI matter.

The DOE CI Program began in 1988 and from its inception through 1996, the Department spent less than \$3.0M annually on CI. In Fiscal Years 1997 and 1998, the Intelligence Committees approved a supplement for the DOE CI budget based on the numerous GAO reports and their continued, significant concerns regarding visitors at the laboratories. This supplement brought the total CI Program funding up to \$6.6M in 1997 and \$7.6M in 1998. Since my appointment in April of last year, I successfully increased the DOE CI budget from \$7.6M to \$15.6M for Fiscal Year 1999 and \$39.2M (which includes \$8 million for CI-Cyber initiatives) for this fiscal year. This very tedious and exhaustive effort was accomplished with the exceptional support from Secretary Richardson and Members from the House Armed Services Committee (HASC), and the SSCI. Without their continued support and push for adequate financing, none of the improvements to DOE's CI Program, which I am about to describe would have been possible. **Direct funding, along with headquarters OCI control and direction of funds to the laboratories and other DOE facilities, is the cornerstone of the 90-Day Study, CI Action Plan, CI Implementation Plan, and an overall effective CI Program at DOE. Without this level of control, meaningful oversight is impossible.** Direct funding has helped us to have greater control over allocation of resources to the priorities I have set for the CI Program. I would like to share with you these programmatic priorities and the efforts OCI is undertaking to improve to the DOE CI Program.

PROGRAM OVERVIEW

First, I will highlight some of the very critical and necessary changes in day-to-day operations of the CI effort at DOE Headquarters. As the result of PDD-61, a new and independent OCI was created that reports directly to the Secretary of Energy. As Director, OCI, the PDD gives me direct CI policy development, implementation and *oversight* responsibilities for all CI activities throughout DOE. The Secretary signed a Delegation Order confirming those responsibilities and delegating to me the appropriate authority to execute them. In addition to my direct reporting and access to the Secretary on CI issues, on a regular, bi-weekly basis, I meet with Under Secretary Moniz or Deputy Secretary Glauthier on CI issues, or as the need arises. Mr. Sanchez, Director of the DOE Office of Intelligence, and I both partici-

pate in these meetings since our offices work very closely together. As the result of the 90-Day Study findings, I determined the optimal OCI organizational structure includes six distinct areas: Analysis, Investigations, CI- Cyber, Training, Inspections, and CI Evaluation Board. Importantly, each of these programs must operate as a single, integrated program; none of them taken in isolation would constitute a viable CI Program.

Analysis Program

The Analysis Program is headed by an experienced Analyst detailed from the FBI with over eight years of specific analytical experience. Her Deputy is also a detailee from the FBI with extensive analytical experience. They both are very familiar with DOE since they participated in the FBI study of DOE directed by the SSCI which I previously mentioned. They have six analysts currently working for them, and are in the process of hiring several more experienced analysts. We expect to place CI analysts at five laboratories this fiscal year. In my opinion DOE has a wealth of information which has not been analytically exploited in the past. The reports we have produced and will be producing are obviously of great importance to DOE but also to the Intelligence Community.

For example:

- A DOE CI analyst played an extremely important role in the preparation of the first annual threat assessment prepared by the National Counterintelligence Center (NACIC) at the direction of the DCI, published on November 27, 1998. This report is required on an annual basis as the result of PDD-61. OCI analysts are currently playing a critical role in the second annual PDD-61 mandated threat assessment which should be published next month. These reports are a direct result of the President's direction and represent meaningful intelligence produced by the Intelligence Community which directly impacts DOE. In my opinion, if it were not for the tenacious efforts of my DOE analysts in this annual effort, the reports would be far less meaningful than they are.
- The Analysis Program has written and will continue to write foreign intelligence threat assessments resulting from DOE's extensive interaction with DOE "sensitive countries." As the U.S. Government's technical advisor to various bilateral and multilateral non-proliferation and arms control initiatives, DOE hosts hundreds of sensitive country foreign nationals each year, and DOE officials are frequent travelers to sensitive countries.
- The Analysis Program is also in the midst of a study of potential economic espionage at the laboratories. The laboratories engage in Cooperative Research and Development Agreements (CRADAs) with private industry. OCI wants to ensure that proprietary economic information is being properly protected.

The projects I mentioned above are expensive but the results and benefits to DOE and the Intelligence Community will allow us to detect and work toward neutralizing foreign intelligence activities being directed against DOE. These products also provide our policymakers with the information they need to make national policy decisions.

Investigations Program

The Investigations Program is headed by another FBI supervisor currently on detail from the FBI with over 23 years experience in Foreign Counterintelligence operations. His primary responsibility is to ensure that any instances in which classified information is being or may have been compromised to an unauthorized party are reported to the FBI. I will continue to staff this Program with qualified and experienced investigators.

CI-Cyber Program

The CI-Cyber Program is headed by an employee from the FBI's National Infrastructure Protection Center (NIPC). The CI-Cyber Program Director serves as OCI's representative to DOE's Critical Infrastructure Protection Task Force. Her daily activities include interaction with DOE headquarters and laboratory computer security professionals, as well as, the NIPC. With the additional \$8 million OCI received for Cyber Programs in Fiscal Year 2000, we are implementing some of the recommendations in the 90-Day Study. For example:

- One of the 90 Day Study's recommendations was the development and implementation of a complex-wide strategy to address the potential CI implications of email to foreign nations.
- As mentioned above, the CI-Cyber Program will significantly enhance the number of CI- Cyber experts this fiscal year in order to further develop field intrusion detection and analysis abilities. CI-Cyber personnel require skills in both computer security and CI.

Training Program

A DOE federal employee heads our Training Program. The purpose of the Training Program is three fold: 1) to formulate an in-house program to train our own CI personnel; 2) to provide professional awareness briefings and debriefings for our scientists traveling to sensitive countries; and 3) to provide awareness briefings for the general DOE population who have an interface with foreigners so they become sensitive to CI related issues. Professional training for CI Officers has been re-oriented to focus on core skills necessary to be an effective CI Officer.

I would like to provide the following examples of our current outreach and awareness training efforts to the DOE population: The OCI currently has a CI professional assigned to the DOE High Enriched Uranium/Transparency Program. This person is responsible for all related CI issues and team briefings and debriefings. He is accepted and trusted as a total team member and the members are willing to discuss sensitive CI issues with him. I have established that same relationship with the scientists and DOE employees associated with the Materials Protection Control and Accounting (MPC&A) Program (the largest program within DOE dealing with the Russians), the Initiative for Proliferation Prevention, the Nuclear Cities Initiative, and the China Arms Control Exchange (CACE) by assigning a CI Officer to each team. Assigning a CI Officer to all such programs within DOE will help us to achieve our goal of briefing and debriefing all DOE personnel traveling to sensitive countries. Our CI goal is not only to protect technology, but also programs involving DOE personnel.

Inspections

We have established an internal inspections process as required by PDD-61. There are two teams available at any given time to complete these inspections. One team is headed by a retired FBI agent who was the former Assistant Director in Charge of the Washington Field Office and was previously the Deputy Director in the FBI's Inspection Division. The second team is headed by a former FBI agent who retired from the FBI as the Special Agent in Charge of the Springfield office and was also an Inspector in the FBI Inspection Division. Both these individuals have over 25 years experience in the FBI and specifically in the CI arena. The Inspection teams are supported by experienced retired FBI and law enforcement officers who are experts in gathering information and resolving complex cases. The teams have been augmented by a senior retired personnel security expert from DOE along with retired DOE laboratory scientists.

As of this date two inspections have taken place—Los Alamos National Laboratory and Lawrence Livermore National Laboratory. A third inspection—Sandia National Laboratories—is underway. All DOE facilities are subject to a CI inspection, and we have scheduled 12 facilities for inspection next calendar year. The results of the first two inspections have been provided to me and the Secretary Richardson. In brief, these results show that significant improvements have been made in the CI Programs at these laboratories since PDD-61 was signed. I will provide summaries of these inspections to Congress in the Annual Report on Counterintelligence and Security Practices at the National Laboratories, as mandated by the National Defense Authorization Act for Fiscal Year 2000. Any significant CI relevant events will be provided to you immediately.

The CI Evaluations Board (CIEB)

PDD-61 authorized the use of many tools designed to reduce the threat to classified and sensitive information at DOE and its field activities. The polygraph was specifically cited as being one of the tools which OCI, in coordination with the DOE Office of Security Affairs, may use to enhance the DOE CI Program. Research and analysis conducted for the 90 Day Study also indicated that the polygraph was one tool that could be used to enhance the effectiveness of the CI Program.

OCI's CIEB is responsible for implementing the DOE CI Polygraph Program. A senior OCI officer is leading OCI's CIEB. I must stress that the Polygraph Program is only one of the six elements of the DOE CI Program; it cannot be considered in isolation. I do not believe that the polygraph is a CI panacea or an infallible CI tool. However, I believe that the polygraph serves as a valuable deterrent to individuals who currently have direct or indirect access to classified information and may be contemplating espionage. I also believe the polygraph serves as constructive screening device for individuals applying for positions requiring access to classified and/or sensitive unclassified information. The polygraph also can be used effectively as an exculpatory tool. The purpose of the Polygraph Program is to protect U.S. national security by attempting to determine if anyone with access has engaged in espionage, sabotage, terrorism, or had unauthorized contact with foreign nationals, or disclosed classified information in an unauthorized manner.

I am extremely sensitive to the anxiety that the Polygraph Program has caused in the Department. I want to stress that we are only going to be administering polygraph examinations to a small percentage of DOE employees having access to the most sensitive "high risk" national security programs. These programs include: Special Access Programs (SAPS), Sensitive Compartmented Information (SCI), Personnel Security and Assurance Program, (PSAPS), and Personnel Assurance Programs (PAPS). The latter two programs involve DOE employees who are involved in the design of nuclear weapons and those who have direct access to these weapons.

OCI has made every effort to reach out to potentially affected personnel to explain the polygraph. Technical briefings for employees of Sandia, Lawrence Livermore, and Los Alamos National Laboratories were held last month. In accordance with the rulemaking process, OCI participated, with General Eugene Habiger, Director of the Office of Security and Emergency Operations, in public hearings. The public hearings were held at:

- Lawrence Livermore National Laboratory, September 14, 1999,
- Sandia National Laboratories, September 16, 1999,
- Los Alamos National Laboratory, September 17, 1999 and
- Washington, D.C., September 22, 1999.

Additionally, as you are aware, I provided a briefing on the Polygraph Program to this Subcommittee on October 4. We also briefed the White House Science Advisor this month.

While DOE has approved a Notice on the Polygraph Program, it only applies to DOE Federal employees. We are currently in the latter stages of an Office of Personnel Management mandated "rulemaking" process to develop regulations for applying the program to DOE contractors. DOE contractors constitute the majority of individuals in the aforementioned "high risk" national security programs.

As DOE participates in the rulemaking process necessary to apply the Polygraph Program to DOE contractors, we have been simultaneously administering the polygraph to DOE Federal employees and volunteering contract employees in OCI and the Office of Environment, Safety and Health. Additionally, some high-level Department officials, including the Secretary, Deputy Secretary and Under Secretary have taken the polygraph. I was the first volunteer to take the polygraph. Overall, approximately 85 personnel have been administered and passed a CI-scope polygraph thus far.

To ensure quality control, the Polygraph Program is managed by an individual that has been the quality control on polygraphs for DOE since 1991. He is the Director of Quality Control for the American Association of Police Polygraph Examiners (AAPP) and the Sub-Committee Chairman of the QC-Committee for the American Polygraph Association (APA). The OCI Polygraph Program Manager also served as the Chief Instructor at the Federal Polygraph School (DODPI) from 1985-1991 and in Government Service Polygraph since 1974. The current DOE Polygraph Program has four layers of quality control; this is more than any other U.S. Government agency which administers polygraph examinations.

Our decisions about who is granted access to classified information must be made with the sole criteria of protecting U.S. national security. The enhancement of the DOE Polygraph Program is not without precedent, as our efforts are bringing the Department in line with the rest of the Intelligence Community insofar as access to "high risk" national security programs are concerned. I believe that the Department's commitment to the overall CI effort is embodied in its support for the Polygraph Program. OCI has received strong support from the Secretary for this initiative, and with his and your continued support we will continue to use the polygraph as an important CI tool.

I am very encouraged about the many initiatives we have begun and accomplishments achieved thus far. While there is work yet to do, I am pleased to say that I have received absolute cooperation from all the senior DOE officials at the laboratories and headquarters. In addition to the senior management support from DOE and the laboratories, I have received nothing but the utmost support and encouragement from Secretary Richardson, Director Freeh of the FBI and DCI Tenet. In addition to showing his support for the CI Program outside of DOE, Secretary Richardson has personally met with the Laboratory Directors and various DOE Assistant Secretaries to reaffirm his support and endorsement of an aggressive CI Program within DOE. This very vocal, personal commitment by Secretary Richardson to an aggressive CI Program at DOE has been paramount to our success thus far. With this continued level of support I am looking forward to appearing before you again to proudly discuss a fully implemented DOE CI Program as mandated by PDD-61.

Mr. UPTON. Thank you very much.

I would just note for the record that all members' statements on both the Oversight Subcommittee as well as Energy and Power will be made part of the record, and I noted that Chairman Bliley came in at one point.

This point we will proceed with questions. I will be pretty strict with this 5-minute rule on the clock. I know that Mr. Cox has already gone to the floor. His bill is on the floor. We have a number of other subcommittees that are meeting as well, and we will start with my questions.

I guess, Mr. Curran, noting your emphasis at the end particularly on polygraphs, there's been a lot of discussion on this for some time. I know you and I talked about it in my office last winter, but—I guess it was in early spring—and where are we on the polygraph?

I noted that Secretary Richardson I think in a very visible way took the polygraph himself to try and illustrate to employees at one of the labs that it was nothing really to fear. There's been a lot of discussion. You talked about that this was a valuable deterrent, only a small percentage of folks, in fact, would be polygraphed. But it's my understanding that so far no DOE employees, other than the Secretary and yourself, but no scientists have been polygraphed; is that correct?

Mr. CURRAN. That's correct, sir. We have polygraphed over 95 Federal employees since the program started.

Mr. UPTON. Are these security people?

Mr. CURRAN. Mostly it is CI people. We required that if we're going to be asking other people to take a polygraph, not just for that reason, because we have access to sensitive information, that all our people will take a CI polygraph. We give an exception as reciprocity for other employees who have received other types of polygraph from the CIA, DOD. We accept that, but CI we do not. We mandate that everybody in CI has to take it.

Mr. UPTON. At what point do you think sensitive folks in sensitive positions, in fact, may be asked to—

Mr. CURRAN. We are—as I said, we are in the final stages. We meet almost daily. We could not legally polygraph contractors unless they volunteered to take that polygraph. We had to go through this rulemaking process where you had the four public hearings. We have concluded that. We have to now respond to the comments in the public hearing which we are doing. Once that is done, then it goes back to the Federal Register, and you have 30 days before you can actually implement.

What we have been doing, because it is such a sensitive topic within DOE, we have been going over each one of these programs with the Secretary, the Deputy Secretary, and, basically, the rule is that we are relying on these people who run these programs, based on the criteria, to tell us who should be polygraphed. We have that list.

Now, we are looking at it and re-examining it to determine are we down to the core, the hard-core people that we want. We're trying to minimize the impact as much as we can, but we still have to address the national security concerns. So I would expect that we would respond to the public hearings, then we have the 30 days in November, and then after that we would start polys.

Mr. UPTON. So beginning?

Mr. CURRAN. December.

Mr. UPTON. December, okay.

Mr. Podonsky, in my opening statement and in your statement as well, there was quite a bit of discussion with regard to the access, particularly from folks not onsite, through computers to information on those computers, the e-mail whatever. You indicated with the Lawrence Livermore that you thought that there were protections from unauthorized access. You indicated that there were some weaknesses. You were expecting some penetration testing used by hackers. At what point do you expect that to happen? December? Do you remember?

Mr. PODONSKY. Yes, sir. In December, as I mentioned, we're going back to all three laboratories. Our biggest concern in the cyber security were the unclassified, and it was not so much from the external penetrations but it was from people who had cleared access from foreign nationals.

We didn't have an issue with foreign nationals. Our issue was if they were from sensitive countries, as we have stated in our classified report, and the potential that those individuals may or may not have to go through the unclassified net into other areas in the unclassified. We had no concern about the classified net. I want to make that clear.

Mr. UPTON. So you feel that the firewall is sufficient on the classified with all of the labs that you looked at?

Mr. PODONSKY. With all three laboratories, we felt that the firewall was sufficient. There are improvements to be made in a couple of the areas, but that would get into some classified area.

Mr. UPTON. Okay. I am watching the clock for me.

Sandia, you indicated, was marginal and it was the rating that you gave them, prompt attention needed. Is that also with regard to the access to unclassified material?

Mr. PODONSKY. To the unclassified.

Mr. UPTON. Why is it that if Lawrence was satisfactory, Lawrence Livermore, and Sandia was marginal, you couldn't get those same type of systems, encourage those same type of systems at Sandia?

Mr. PODONSKY. Mr. Chairman, are you talking about the overall rating?

Mr. UPTON. Yeah. Your overall rating. I presume—well, you tell me—by giving a marginal rating at Sandia tells me that there's some obvious weaknesses there. Were some of those weaknesses in regard to access to unclassified information through the computers?

Mr. PODONSKY. Relative to all three sites, Los Alamos receiving overall satisfactory, the other two labs received overall marginals, but all of them received less than satisfactory in the unclassified cyber security because of weaknesses on the access of the internal approved individuals. For example, there are different tiers of an unclassified information. Some of it is sensitive, and we had the concern in terms of what kind of administrative controls were on at actually all three laboratories.

Mr. UPTON. I will follow up when we come up.

Mr. Stupak, do you want to go next?

Mr. STUPAK. Sure. Thank you, Mr. Chairman.

I apologize for being late. I just got in from Michigan, dealing with DOE no less.

Mr. Podonsky, if the laboratories can reach satisfactory rating without more money, can you tell us why we should give them more money? Either they're satisfactory or they're not. Or are you just determined, as the General said that they have, and I am quoting his testimony, foundation to perform their security functions capably given adequate resources? So do you really need the money or are you playing off that statement?

Mr. PODONSKY. When we assign a rating that we believe that the individual site earns, it's based on their performance. A satisfactory rating does not mean that everything is perfect. It does not mean that there are not other management areas needing attention. Relative to resources or money, I would yield to the policy arm as well as the lead PSOs as to what moneys they do or do not need. When we look at it, we try to not look at programmatic needs. We look at strictly how effective the policies are being implemented or not.

Mr. STUPAK. If you're going to give a satisfactory rating, I don't say on appropriations, obviously, but I am sure the Congress would be probably hard pressed to give more money to an agency that's doing satisfactory work, and if it's satisfactory, how would you make the case to the appropriators that you need more money?

Mr. PODONSKY. Well, specifically if we take Los Alamos, there are many upgrades that are still needed regardless of the fact that they have received a satisfactory rating. Satisfactory is not the penultimate that we walk away from and say everything is fine. In the case of cyber security, unclassified, as I mentioned to the chairman, all three laboratories need extensive work in this area. So, obviously, there would be funds necessary—

Mr. STUPAK. What was the last rating of Los Alamos?

Mr. PODONSKY. The last overall rating, it was just rated in August as satisfactory.

Mr. STUPAK. And let me take it one step further. The last time we had a hearing here, it seemed to me we gave—there was a special line, \$5.3 million I believe the number was—I am going off the top of my head, so I may have the number wrong. That's supposed to be for security, but two-thirds of that money went for administrative costs and administrative travel. What guarantee do we have that even if we gave you more on top of a satisfactory rating, that it is really going to go to this security upgrade that you need?

Mr. PODONSKY. Well, one point of clarification that I need to make, on the satisfactory rating, it may in fact also be because of compensatory measures which are short-term fixes, not long-term. So there are long-term fixes at all three of the sites. We add an oversight element of the Department. We cannot give you the guarantees that the moneys are going to be used appropriately. All we can do is report back on how effective the security is, and we report it back to the Secretary and to the lead PSOs.

Mr. STUPAK. So you don't oversee the security operations then?

Mr. PODONSKY. We oversee the security operations. We oversee the security implementations of improvements, but we don't oversee the security budget. That's General Habiger.

Mr. STUPAK. Sure. Okay. So you're the oversight. How much pressure do you have as oversight to get these security measures implemented in a timely, cost-effective manner?

Mr. PODONSKY. When the Secretary elevated our office to directly report to him, our responsibility was to go out and kick every stone, turn over every piece of information, find out where the vulnerabilities or the strengths were. But, at the same time, the Secretary encouraged us to work with the policy folks as well as the lead PSOs to help find solutions. Our main thrust as we provide information to the Secretary and to the Congress is how effective the policies are being implemented. The pressures that we have are strictly that the Secretary wants to make sure, as I am sure the Congress is, that there are no security problems in the department.

Mr. STUPAK. Speaking of your oversight roll in that, you're supposed to be independent of the rest of the security bureaucracy, are you not?

Mr. PODONSKY. That is true.

Mr. STUPAK. And you're supposed to be independent of General Habiger, and you don't report to him, do you?

Mr. PODONSKY. No, I do not.

Mr. STUPAK. Okay. Then who do report to?

Mr. PODONSKY. I report directly to the Secretary of Energy.

Mr. STUPAK. Okay. You're supposed to be the outsider in this whole thing to give your recommendations, right?

Mr. PODONSKY. We are supposed to give an unbiased, unfiltered, independent look at how effective the Department is implementing its policies, how effective its policy is and report that back to the Secretary, report it to the lead PSOs. We're the outside, independent, internal group.

Mr. STUPAK. Well, in the General's statement, he says, and I am quoting now, Glenn and I are working closely together to ensure an integrated approach through policy development and oversight. Well, you're supposed to be doing oversight, not policy development, right?

Mr. PODONSKY. We do not develop policy.

Mr. STUPAK. Okay. Well, that statement would indicate an integrated approach to a policy development oversight, so I want to make sure that you're truly independent and that we're developing security with an independent look at it and not back into the culture of DOE which has neither been accountable nor accept responsibility for past breaches at DOE.

Mr. PODONSKY. I can't answer for the General, but if you indulge me—

Mr. STUPAK. Sure.

Mr. PODONSKY. One of the major changes that have occurred in the last year, and I have been with the Department for 15 years, is that the security infrastructure that the Secretary set up is working together. In the last 15 years, it was not always so. For example, we do not develop policy, but we evaluate the effectiveness of that policy. In previous years, we would inform the policy people of our concerns about some of the unclear policies. Oftentimes, we had disputes and with no resolution.

What General Habiger, I believe, is inferring is that we now have an infrastructure where when we provide information directly to the General and his people. We're seeing corrective actions. We're seeing an adult dialog, which has not been the norm of the Department.

Mr. STUPAK. From where we're sitting, and it seems like maybe too much of a cozy relationship in that I think—and I don't speak for all of the members—but I always thought your idea would be to have General Habiger write policy and implement it and then it was your job to see that it got done.

Mr. PODONSKY. That's what we're doing.

Mr. STUPAK. Okay. Just from the statements there it sort of looked it's not really what's going on, maybe too close of a relationship. And I want to make sure that, you know, the General's shop is not determining how oversight should be done, but that really should be on your side and be independent thereof.

Mr. PODONSKY. Just as an illustration, the General has a number of findings in our reports that he's responsible and his office is responsible for providing corrective actions to.

Mr. STUPAK. Thank you.

Mr. UPTON. Mr. Burr.

Mr. BURR. General, welcome. Glenn, good to have you here again. Mr. Curran, also good to have you.

Mr. Curran, you mentioned polygraph 27 times. The General mentioned it once. I don't think Mr. Podonsky, unless I missed it, mentioned it. Polygraph was one of, if not the biggest initiative that the Secretary announced in his revelation that we had a problem. He conveyed not only this Congress, but to America that it would start the next day. To date, 85 people, if your first statement was correct, 95 if your second statement was correct, have been given the polygraph. They are CI individuals. They are the Secretary, they are the General, and they are you. To date, no DOE employed scientist have been given a polygraph; am I correct?

Mr. CURRAN. Correct.

Mr. BURR. Do you need further policy directives to have the jurisdiction to administer a polygraph to DOE employees?

Mr. CURRAN. Contractors?

Mr. BURR. DOE employees.

Mr. CURRAN. No.

Mr. BURR. You do for contractors?

Mr. CURRAN. I don't need any further regulation for DOE Federal employees, correct.

Mr. BURR. And are there Federal employees that you intend to administer a polygraph to?

Mr. CURRAN. All Federal employees assigned to my office have been polygraphed.

Mr. BURR. Is there anybody in the lab structure that is a Federal employee?

Mr. CURRAN. That has not been polygraphed, no.

Mr. BURR. Have all the managers of those facilities that are deemed DOE employees been polygraphed?

Mr. CURRAN. Some of them, not all of them.

Mr. BURR. Not all of them. Do you intend to polygraph the other ones?

Mr. CURRAN. They would—they would come under the matrix to be polygraphed.

Mr. BURR. But they have not been done yet?

Mr. CURRAN. Have not.

Mr. BURR. You also made the statement that we're relying on the individuals that run these programs to tell us who should be polygraphed; is that correct?

Mr. CURRAN. That's correct.

Mr. BURR. Are these the same individuals who have had the responsibility to oversee security at these facilities?

Mr. CURRAN. No. There's a catchall there, also. The manager who runs a specific SAP program or is required to provide me with a list, based on the criteria that I give him, of who he thinks should be polygraphed. I then have the option to disagree with the manager's decision.

What we're asking is to work this as a concerted effort at this point, since these people know more about the SAPS and the PSAPS than I do, but we have the authority to go back.

Mr. BURR. Do you agree that the intent to polygraph, as far as the size of the population based upon where the Secretary originally made statements from than what it is today, has been reduced significantly?

Mr. CURRAN. No. The rulemaking process that we have just been through covers all the areas that I identified in the PDD report. That's the total population.

Now, I have said right from the beginning I do not believe that all those people involved in those programs need to be polygraphed. That's why we're in this process now. For example, a SAP program has different layers of access, Tier I to—one's in administrative access; one's a technical, which is the most critical; and one's a security.

Now, in some SAPS, we may say everybody gets polygraphed. In other SAPS, we might just say Tier III people get polygraphed. That's what we are looking for the program managers to help us out with. But they're not deciding what the criteria is. We are. We're working with them to do that.

Mr. BURR. Well, clearly, if program managers had their choice, the answer would be none.

Mr. CURRAN. Excuse me, sir?

Mr. BURR. If the program managers had their choice, I think the answer would be none.

Mr. CURRAN. I have been meeting with the Secretary and the Under Secretary almost daily for the last 3 weeks. They have come up with a number that is pretty close to what we had originally. I can honestly tell you the program managers in these programs have been very, very cooperative.

Mr. BURR. I wait curiously to see what your number is and to go back and read the Secretary's statements when he made it about how many people he sought to be administered polygraphs.

General, I need to ask you a question, and I hope you will take this in the spirit that I ask you. Who wrote your testimony?

Mr. HABIGER. Who wrote it?

Mr. BURR. Yes, sir.

Mr. HABIGER. I wrote 90 percent of it, sir.

Mr. BURR. Ninety percent of it. The part about the budget, did you write that?

Mr. HABIGER. Yes, sir, I personally wrote it.

Mr. BURR. You personally wrote that.

Mr. CURRAN, have you ever been denied of any of the resources you have requested?

Mr. CURRAN. No, I have not, sir.

Mr. BURR. Let me give you a description of what the Budget Committee said about the \$35 million requested for DOE, which was emergency money, I think either slightly before or upon your arrival that I'm certainly not tagging to you. I won't use the word, but it's four letters. It started with C-R and ended in A-P.

They asked for that request to go back and for there to actually be specifics tied to it as far as what it was going to be used for.

Now, we've got one of the gentlemen who will testify in a minute, Mr. Weigand. He's the Deputy Assistant Secretary for Research and Development. He says we have committed an abundance of resources to fix the problems and to date have reprioritized funding within our existing budget.

Let me ask you, General, can this be reprogrammed and meet our needs? I think there's currently \$800 million that is devoted to security. Or will the Congress have to appropriate new funds within DOE to meet this need?

Mr. HABIGER. Sir, let me make this very clear. When I took this job, I asked the Secretary to do two things: No. 1, allow me to work directly for him. Done. No. 2, I told him I couldn't do the job without having absolute total control over the \$800 million. We're in the process of doing that. We're going to be working with the appropriations committees and authorization committees. For the fiscal year 2000 budget, we're tagging the money. I have oversight over security dollars in the fiscal year 2000 budget.

The fiscal year 2001 budget, which will be coming over to the President in early February, the money will be broken out, stripped out under a different appropriation, be titled security. I'll be accountable. I'll be responsible. We're going to spend it in the right place.

Mr. BURR. I feel very confident that your intentions are, in fact, correct. One of the hesitations of this committee has been I think a thing that Mr. Podonsky and this committee share, that we have been in the process a heck of a long time, and I hope in the next 5 minutes, Mr. Chairman, in the next round we will be able to ask some more questions.

Mr. UPTON. We'll do so.

Mrs. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman.

I have a number of questions with respect to computer security, and I don't know, Mr. Curran, if you're the correct one to address these to. If not, these others chime in.

I understand that you have conducted security reviews at the national laboratories. What other DOE facilities have you conducted cyber security audits on?

Mr. CURRAN. That's more a function—

Mr. PODONSKY. That would be more in our area, ma'am.

Mrs. WILSON. Okay.

Mr. PODONSKY. We just finished an inspection at Oak Ridge at Y-12 facility.

Mrs. WILSON. Have you ever conducted an audit on DOE headquarters?

Mr. PODONSKY. We did, in 1991.

Mrs. WILSON. Have you conducted one within the last year, 2 years?

Mr. PODONSKY. No, ma'am, we have not.

Mrs. WILSON. Are there connections between the DOE headquarters or DOE Germantown computer systems and the national laboratories, either through wide area networks, client servers or anything?

Mr. PODONSKY. I believe there are.

I was just told, no, there is not.

Mrs. WILSON. There are no computer links between Germantown or DOE headquarters and our national laboratories?

Mr. PODONSKY. There is communication links between, and it varies. There's classified networks—

Mr. Chairman, may I introduce the director of the Office of Cyber Security?

Mr. UPTON. I think you should, and we probably need to give him the oath, too. We will stop this clock here. I don't know that we'd be such good 2-minute coaches here, 2-minute drills, but if you could state your name for the record.

Mr. PETERSON. My name is Brad Peterson.

[Witness sworn.]

Mr. UPTON. You may proceed in answering that question.

Mr. PETERSON. The headquarters network is linked between Forrestal and Germantown as part of one DOE headquarters network. As far as a wide area network with other fields, as far as, you know, linked into one network, no. There is, of course, Internet connectivity. As far as on the classified side, there is a capability to send classified e-mail back and forth over an ES net, but it goes through NSA encryption as it leaves one site and would go through encryption on the other side as it would come out.

Mrs. WILSON. Thank you.

Mr. Podonsky, obviously the question that I am getting at here is the weakness of the computer system is only as strong as its weakest link, which means checking the laboratories themselves. That alone is probably insufficient for cyber security services, and I wonder if you could tell me what your plans are for auditing of DOE headquarter systems.

Mr. PODONSKY. Currently, Mr. Peterson, our office director, is working with John Gilligan, who's our CIO, in looking at the overall implications of what we are finding in the field and bringing it back to the national look. For example, there were just—the unclassified computer security order is just being put out now. It's been an issue that we've had for quite some time.

Mrs. WILSON. Let me interrupt you here. When do you plan to do an audit of DOE headquarters or Germantown's systems or is it just not on the schedule?

Mr. PODONSKY. No. It's on the schedule for next year.

Mrs. WILSON. Thank you.

When you did your review of the national laboratories, were you able to penetrate the classified systems from outside of the fence—I mean, from offsite?

Mr. PETERSON. No, we weren't, ma'am. Their systems are air gapped, so you cannot actually gain access.

Mrs. WILSON. Were you able to penetrate the unclassified systems? And, if so, what kind?

Mr. PETERSON. We were able to penetrate the unclassified firewall at Sandia. However—

Mrs. WILSON. What kinds of systems? Was it personnel? Was it—what kinds of systems were you able to penetrate?

Mr. PETERSON. We were able to gain access to different servers. Our time we test is very limited, so we did not fully explore how far we could migrate through the system. At Sandia—

Mrs. WILSON. Was it the personnel computer? Was it the telephone controller? What did you penetrate? Or if you can't do it in an unclassified forum, I understand.

Mr. PETERSON. It was a regular computer that might be sitting on a researcher desk type of a thing so you can get some types of files.

Mrs. WILSON. So you penetrated researchers' computers at the national laboratories?

Mr. PETERSON. That was—and, again, this is probably something we should wait and go into at a different level to be able to answer your question fully. It's not appropriate in an unclassified environment.

Mrs. WILSON. Thank you.

I think we can probably answer this question in this forum. If you hired the same hackers, Mr. Podonsky, or contracted with them or conducted them to penetrate your computer on your desk or my computer on my desk, do you think they could do it?

Mr. PODONSKY. I think, without worrying about damage to your software or mine, yes, ma'am.

Mrs. WILSON. Thank you.

Mr. UPTON. Mr. Cox.

Mr. COX. Thank you. I have got a handful of notes from staff who are trying to keep track of what was said. I apologize for my absence, and I also apologize if I cover any ground that's already been covered. I think I have a good idea of which topics were covered, and I will try not to be repetitive.

Just as an overview, since you are all DOE employees, the President's Foreign Intelligence Advisory Board, as I mentioned in my opening statement, said the Department of Energy "has had a dysfunctional management structure and culture that only occasionally gave proper credence to the need for rigorous security and counterintelligence programs at the weapons labs." That report, as you know, was as of mid-year 1999. Does any of you disagree with that? Anybody care to disagree with that?

That's a pretty harsh assessment, and it is as of the middle of this year. It gives rise to the question why, if we are looking for something systemic here, did it take 20 years for the Department of Energy to come up with a counterintelligence plan? And I guess, Mr. Curran, since you have been tasked now with that—

Mr. CURRAN. If I can answer your question.

Mr. COX. We didn't even have an Office of Counterintelligence created by the direction of the Secretary, then Secretary Pena, until 1998. Why did it take so long?

Mr. CURRAN. I can't answer the whys to that, sir.

I think in my opening statement we confirmed exactly what you did say. I mean, there was not any counterintelligence program within DOE that even met minimal standards.

I am not a DOE employee. I am an FBI employee detailed to DOE. Since my initial 90-day study and the implementation plan, I can tell you that I have received outstanding cooperation from the senior management in the three weapons labs. I don't think we could have made the progress that we have made without their cooperation. The CI inspection process looks at executive management and their role and participation in a CI program. And if we don't have that, the program's not going to work. So I think we do hold their feet to the fire on that. I know the Secretary does.

Mr. COX. I know that there's been some discussion during the members' questioning of polygraphs, and so I'm going to be as brief as I can because I don't know exactly what was said, and I don't want to ask you the same questions over again.

But, Mr. Curran, in your testimony you said that the plan for polygraphing is modelled on other intelligence agencies. Using the CIA as an example, what's your understanding of CIA's policy?

Mr. CURRAN. As you know, Mr. Cox, I served for 3 years out at the CIA, post Ames, and one of the problems I faced was the fact that they had an exorbitant number of people who had failed the CI polygraph. They went back after Ames and retrieved all the charts in the hundreds. That's what I was faced with when I got there. Now, obviously you don't have that many spies in the agency. There was something wrong with the program, in my opinion.

The counterespionage group that I ran at the CIA determined that we need to revise the polygraph itself. CIA has a lifestyle polygraph, the general polygraph. What I was interested in only was if the person was a spy or not. We were able to bring down the focus of the polygraph. The more focused the polygraph is, the more successful it is. The wider it is, the less useful it becomes.

And basically we came down to two questions. When we asked a CI employee, have you ever passed on—have you ever had unauthorized disclosure of classified, they all flunk it. I mean, because that's their business. They are in that on a daily business.

But if you ask them, have you illegally passed classified information to a foreign agent? Do you know what I mean? We were able to resolve—of the hundreds of cases we had, we resolved 85 percent of those that we said, hey, this person may have other problems, but the person is not a spy. They may have to pay their income tax for the last 10 years, but that's how we were able to get through that.

Mr. COX. What you're outlining is a distinction between the proper administration and use of this tool on the one hand and the universe of people to whom the test is applied. Particularly with respect to the latter, what do you understand CIA's policy to be?

Mr. CURRAN. All employees of CIA get a lifestyle polygraph.

Mr. COX. Would that include a secretary?

Mr. CURRAN. Yes, all employees.

Mr. COX. So the night watchman?

Mr. CURRAN. Yes. I think it excludes the gardener. I am not quite sure.

Mr. COX. Now at DOE, as of today, as we meet here, is there any nuclear weapons scientist who has been polygraphed other than in the course of a law enforcement investigation?

Mr. CURRAN. As far as I know, there has not been. Now, I think there's an area that we can go into that I don't think we should go into here where because of what that person can maybe do and may have been polygraphed, but I think 99 percent, no.

Mr. COX. My red light is on. Is my time expired? That's usually what it means.

Mr. UPTON. I indicated earlier that we wouldn't make very good 2-minute drill football coaches, unless you play for Notre Dame. They had a little trouble at the beginning of the year.

We'll start the second round of questions. Just for the record, too, Mr. Peterson, if you could give your title.

Mr. PETERSON. Director of the Office of Cyber Security and Special Reviews within the Office of Independent Oversight and Performance Assurance.

Mr. UPTON. Thank you.

Based on that, I don't know if this question would be more directed to you or Mr. Podonsky. But, as I understand it, that in the past the inspections in fact have found—even though there's a fire-wall that's been identified for access to classified information, in fact, as I recall, some inspections showed that classified information was on unclassified systems. Isn't that correct?

Mr. PODONSKY. The short answer to that is, yes, when we were doing some penetration tests a year ago that we did find on the unclassified one or two documents that were deemed to be classified by the Office of Classification.

Mr. UPTON. Has that been corrected? I know, I think in the Wen Ho Lee case that was indicated that he perhaps wittingly or unwittingly had transferred many, many lines, thousand perhaps, of classified on to the unclassified. Is that still—is that allowed? Is that possible?

Mr. PODONSKY. We have not found that during this round of inspections.

Mr. UPTON. And you would agree that if that was still possible, though, one could navigate and, in fact, get classified information on that unclassified system; is that not correct?

Mr. PODONSKY. If that is still possible, that is correct.

Mr. UPTON. I understand that each of the labs permit foreign nationals from sensitive countries, whether it be Iran, Russia, to have authorized user status on their unclassified systems, both onsite and via remote dial up. Is that correct? And, if so, how many folks would that be?

Mr. PETERSON. We would have to defer to the laboratories for the specific numbers, but it's our understanding that both Lawrence Livermore and Los Alamos have individuals from sensitive countries, foreign nationals from sensitive countries with remote access, including at Los Alamos one from Iran. At Sandia, to our understanding, there is no foreign nationals from sensitive countries with remote dial up access.

Mr. UPTON. There are none at Sandia?

Mr. PETERSON. Yes, sir.

Mr. UPTON. Is that possible that's going to happen at all three labs? I mean, is that a goal and is it anticipated to happen soon?

Mr. PETERSON. I do not believe so, sir.

Mr. HABIGER. Mr. Chairman, if I may?

Mr. UPTON. Yes.

Mr. HABIGER. Podonsky discovered the problem at Los Alamos in August. We have got policy that should have been out a week ago, but because of some legal verbiage, we will have policy out within the next 5 days that will greatly tighten this foreign access. And I think with your experience with the Department of Energy you could say this is unprecedented, to get policy out that quickly.

Mr. UPTON. Will it be prohibited with this new policy that will be in place?

Mr. HABIGER. No, sir. We have gone to the labs. We got their inputs. There are certain treaty implications that give foreign scientists access into some of our systems.

Now, let me point out, we have to look at the different tiers of access in terms of the national laboratories versus a Brookhaven where we have medical research that's going on. We have scientists out there that need access to that kind of information, but the control and the approval will be at a very high level at the lab sites—so that there be accountability, and the security plans for each of these individuals—and there will be a security plan for each individual—will be brought to bear before that individual has access.

Mr. UPTON. What about access to some of these weapon parts that are at these sites? How would you describe the protection of those parts that might be, I don't want to say lying around, but stored at each of those sites. I don't know who would have, Mr. Podonsky.

Mr. PODONSKY. At all of the sites we had issue and concern about classified matter, classified parts. What we have found is that all the sites did take corrective action. For example, Los Alamos had over 105 different locations that are now down to 41 sites. They needed to be inventoried. They needed to be put into smaller storage areas so that they could be better protected. And if I am not correct, I do believe that all three sites have taken corrective actions, but we'll have a better feel for that in December when we go back to see how far they went.

But relative to what type of access, we didn't see when we were out there that other folks had access. We were concerned about the potential of the vulnerability of the parts where they were stored.

Mr. UPTON. And what types of parts would they be that you looked at 41 different sites within one site? I mean, you're talking about cruise missile—what type of parts are you—

Mr. PODONSKY. Well, it varied at the different sites. At Los Alamos, it was very nonnuclear weapon components, an array of shapes. At one site earlier in 1998 there were cruise missiles, as you started to mention, but that was put into locked storage.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. Podonsky, where does your office go if the Department puts its weapons facility into a new semiautonomous agency?

Mr. PODONSKY. That's not clear, sir. As far as we know, we still work for the Secretary, and if we fall into that nebulous area called Secretary staff to oversee the new agency, but there is no clear indication where that would be. It's my understanding in talking to the Secretary that that would be his intent, is that we would be the oversight arm for that new agency.

Mr. STUPAK. So you'd still see the weapons facilities operations then.

Mr. PODONSKY. That's our understanding, but right now the devil is still in the details, and we haven't seen all the details yet.

Mr. STUPAK. But that's only if the Secretary's plan is approved as he's laid out for us?

Mr. PODONSKY. That's as much as I know.

Mr. STUPAK. Okay. What would happen if there is any oversight?

Mr. PODONSKY. My personal opinion is it's kind of like the formation of the entire Federal Government, executive branch and legislative arm. It's based upon oversight existing—and my belief is that there's always going to be a need for an independent arm to just be a wake-up call, a reminder for the various elements in the Department or the new agency.

Mr. STUPAK. One of the lab's responsibilities is to protect special nuclear material, isn't it?

Mr. PODONSKY. I am sorry, sir?

Mr. STUPAK. One of your responsibilities is to protect special nuclear material.

Mr. PODONSKY. The Department's responsibilities, yes.

Mr. STUPAK. One of the lab's responsibilities?

Mr. PODONSKY. Yes.

Mr. STUPAK. We're going to hear later today that one of the labs has consistently met measurement inventory requirements for special nuclear material, but you told the staff a few weeks ago that Livermore has not been able to do measurements for a long time. Mr. Weigand has now said new procedures have been put in place to, quote, inventory different system analysis, end of quote, and that the reference material has just been acquired to measure uranium holdings. So has Livermore consistently met these measurements in inventory requirements?

Mr. PODONSKY. Not in the past, no, sir.

Mr. STUPAK. Where are they now then? Are they meeting it now?

Mr. PODONSKY. My understanding from my inspectors, yes, that they are moving forward in their material control accountability program. This is another area that General Habiger and his folks are going to need to take a look at across the complex in terms of the dealing of different materials that are difficult to measure.

Mr. STUPAK. Well, if they're doing it now, how are they able to measure it now? Is that because they have new equipment? Have they done a reinventory?

Mr. PODONSKY. When we were out there, they had committed that they were purchasing new equipment. My understanding is that's where they are moving toward. Again, I want to emphasize, we're going back out there in December to see the progress that have been made.

Mr. HABIGER. Sir, if I may, one of the organizations that works for me now, the New Brunswick laboratory, is responsible for get-

ting some measuring isotopes out there. I was out at Lawrence Livermore here about 2 months ago. They told me that they could not go green, complete their material control and accountability by the end of the year unless they got that measuring standard. We pulled out all the stops, got the stuff there. It's there. They are in the process. They'll be fixed by the end of the calendar year.

Mr. STUPAK. So what did they do before then if they didn't have the equipment to do it?

Mr. HABIGER. They were—I am talking about one specific item that I was responsible for, but there's—part of the problem, and I am not going to go into a lengthy explanation, is that when you do inventories, let us say you did an inventory in 1991, you used a set of equipment. Then you did another inventory in 1995. Things looked okay using the same set of equipment. Then you bought a third set of equipment and higher technology, closer measurements. You have a delta in the amount of material. Then you have to go mitigate, figure out did you actually lose some or is it just the measuring standards. And that's part of the issue that I am most familiar with.

Mr. STUPAK. We don't have an answer yet on that part. We're still trying to figure out what happened there then for the discrepancies in the numbers then?

Mr. HABIGER. Yes, sir. And we're talking about very, very small bits.

Mr. STUPAK. That would be small bits of like plutonium?

Mr. HABIGER. I cannot answer that for you, sir. I will have to get back to you.

[The following was received for the record:]

The Department is confident that the discrepancies in inventory values at LLNL are not caused by actual losses of nuclear material but, instead are caused by measurement errors. A known source of these errors is the inability to accurately measure these materials (Highly Enriched Uranium). In the past, LLNL's inability to accurately measure portions of their inventory has been due to a lack of new measurement technologies and measurement standards. Recently, LLNL has acquired new technologies and measurement standards for use in their measurements program.

With these new capabilities, LLNL and the responsible DOE offices have committed to performing all required measurements related to their nuclear material inventory.

Mr. STUPAK. Okay.

Mr. Podonsky, do you believe that problems at the labs are particularly DOE's fault because their directives were ambiguous or completely lacking?

For example, Sandia brags that it has a world-renowned security expert, but it didn't know enough to set up the secure password systems on its computers. So whose fault would that be, DOE's or the world-renowned lab?

Mr. PODONSKY. If you indulge me for a moment, I'd like to answer that. There's a lot of fault in terms of the security posture of this Department. Having spent 15 years inspecting and producing over a hundred classified reports, I would tell you that many of these issues, with the exception of the potential espionage—alleged espionage case we have identified, it's a matter of attitude and accountability. That's both on the Federal side as well as the contractor, be they lab or be they M&O contractor.

We have seen cyclical periods in which the Department has focused on environment safety and health, security, back to security, back to environment safety and health. What we are seeing now is something starting to hopefully take hold, and that is that everybody has a responsibility, be it a safety or security responsibility. There is no question that there's expertise at the laboratory as well as within the Department. None of these issues that we have seen over time is, we call it, rocket science. A lot of responsibility rests with everybody that's involved in the Department, be they contractor or—

Mr. STUPAK. I don't disagree, but, you know, I asked just a question on passwords, who really would have the responsibility there, and we always seem to get back to the questions about, well, you know, it's the culture, there's been no accountability, there's been no responsibility, but it keeps going on. So, when you're going back from environment to nuclear to whatever it might be, if it's the same old culture, we don't break that cycle, it's going to continue, and we're going to be back here a few more years later.

And when I asked the questions earlier about you and the General being cozy on your relationship of policy and implementation, I wasn't trying to do it in a negative light, but we've got to break that cozy relationship if you're really going to get some answers here. And so like I just took a simple example like passwords on the systems for the computers, who would responsible, DOE or the labs themselves. I guess that's what I'm trying to show, to break this up here, so we get some responsibility, so we have some accountability so we can change this culture.

Mr. PODONSKY. What we have seen—and I wish to reiterate this point—is that we have seen that the M&Os are taking the responsibility, the line in the Department is taking the responsibility, the policy folks. And I also want to emphasize, working together is important. Because there is such fragmentation within the Department, that also calls for confusion of what policies were meant to be implemented, what was expected, as well as what the expectations were for the various contractors.

Mr. UPTON. Okay.

Mr. STUPAK. I know my time is over. I appreciate it, Mr. Chairman, but I just—I even go back to the password. Someone has to know they need a password. I mean, that's pretty basic.

Mr. HABIGER. Mr. Chairman, if I could, 15 seconds.

Mr. UPTON. You got it.

Mr. HABIGER. Mr. Stupak, I am accountable—I'm responsible for policy, and one of things we found, we didn't have a policy for passwords. Within 10 days, we'll have policy out in the field for passwords.

Mr. STUPAK. I wouldn't think that these world-renowned labs would need a policy that you have to have a password to get into a computer. Good grief, the basic level in my office know that.

Mr. UPTON. Mr. Cox.

Mr. COX. Thank you, Mr. Chairman.

Mr. Podonsky, I'd like to just ask your help in understanding some of your findings. There's already been some Q and A about classified parts. In your view, are the inventory problems fixed at the labs?

Mr. PODONSKY. In our view, they are on their way to being fixed at the labs.

Mr. COX. That's different than they are fixed, I take it?

Mr. PODONSKY. Well, we would like to see—we would like to see more, but we are pleased at the progress that has been made thus far.

Mr. COX. So they're better than in 1998 for example?

Mr. PODONSKY. Yes, absolutely.

Mr. COX. This cruise missile incident that the chairman mentioned was fall of 1998; is that right?

Mr. PODONSKY. That was in 1998, yes, sir.

Mr. COX. Now, I take it that the external aspect of the cruise missile is not classified so that photographing it from the other side of the chain link fence—where it was visible—would not have been a breach of the classification?

Mr. PODONSKY. I'm not aware as to what parts of the missile would or would not be classified.

Mr. COX. What can you tell us about that incident?

Mr. PODONSKY. One of my inspectors found a number of—number—3 or 4, I am not sure, I don't recall which—of cruise missiles that were being stored, and we felt that they were not in a secure environment. If I'm not mistaken, they were stored outside—they were stored inside a block building, but there was no protective force that we could see during the inspection. Now, since then, all these parts have been put into a secure environment.

Mr. COX. I take it the problem with classified parts is one that's gone on for a number of years?

Mr. PODONSKY. Yes, sir.

Mr. COX. If I understand your report correctly, you raised concerns about Los Alamos' protection strategy in 1994?

Mr. PODONSKY. As far back as 1994, yes.

Mr. COX. In your 1997 report on Los Alamos, 3 years later, you stated that the lab received clear direction from the Department and its field office in 1995. Now, that 1995 direction would have come a year after your 1994 report finding problems, that Los Alamos received clear direction again in 1996 to fix its problem with classified parts protection, and that when you returned in 1997 you found that the situation, "remains essentially unchanged since 1994." So we've got 1994, 1995, 1996, 1997, 4 years where there's a clear signal going to Los Alamos to fix the problem, and in your estimation, nothing happened; is that right?

Mr. PODONSKY. Yes, sir, that's a correct characterization.

Mr. COX. Since you have been around this, do you know why that would be?

Mr. PODONSKY. I can only give you my personal opinion, but relative to—relative to the focus at that time, I would defer that to line defense programs and the laboratory to explain why that reoccurred.

Mr. COX. I take it that if you don't have a good inventory system for classified weapons parts, that creates an immediate problem because you don't know when a piece has gone missing; is that right?

Mr. PODONSKY. You have a potential for that.

Mr. COX. And so when it then comes to questions of adequately securing those parts, in other words, they're not guarded properly,

we don't know whether in consequence of this long-running problem, that at Los Alamos we have said recurred throughout 1994, 1995, 1996, 1997, whether or not something was stolen and we no longer have it; is that right?

Mr. PODONSKY. You could infer that. We have no evidence that anything was missing. We were concerned about the practice.

Mr. COX. But, of course, you don't have an adequate inventory either.

Mr. PODONSKY. No, they do not.

Mr. COX. Let me ask you about the Superblock. This is the area at Livermore which we are most concerned about from a security standpoint, I would take it, because that's where we store our nuclear material. Now, your report tells us that we had a guard force that I take it was adequate in 1995. Was it adequate in 1995?

Mr. PODONSKY. They started to go through some reductions. Adequate training, yes. Adequate numbers—

Mr. COX. From 1995 to 1997 your report says that guard force got cut almost in half. Why did that happen?

Mr. PODONSKY. The Department was going through reductions in attempts to save, save money.

Mr. COX. In your view, is that a good place to save money and a good way to save it?

Mr. PODONSKY. It was never our view, no, sir.

Mr. COX. You describe the measures that have been taken to upgrade that security since you pointed out the deficiencies as temporary, pending permanent fixes. What is the nature of the temporary fix compared to the permanent fix that you expect?

Mr. PODONSKY. Without getting into classified because of the open session, we are working to—we are following what they are doing in terms of their testing. What's of critical concern to us is their ability to perform against various scenarios. They have, to their credit, have increased the numbers of guards at the Superblock. The next piece of it is going to be their ability to protect assets they are assigned to.

Mr. COX. Given that you have been around this block several times, around the Superblock, given that you've had to write reports in successive years pointing out that nothing has changed, when we hear that fixes are pending, that, for example, the accounting problems are not solved, parts of accounting problems are not solved but they are on their way to being solved, that the temporary fix is in place for the nuclear material guard force, will be made permanent, what can you tell Congress that will assure us that this time it's different?

Mr. PODONSKY. I have served through four Secretaries. I have reported to many congressional committees. It's only in this last year that I have seen a Secretary of Energy fully engaged and a Congress fully engaged to follow through on many of the issues that we have identified over the years. So I and my people feel very confident, albeit somewhat guarded, that there's so much attention being paid that perhaps now we will finally get there. We know the Secretary is committed. We know the Department is committed. I know that my colleagues that report directly to the Secretary, such as General Habiger, is committed. We haven't seen that before.

Mr. COX. My time has expired I see, and I don't want to test the goodwill of the chairman.

My understanding is that you're gone in a year; is that right? Well, I'm sorry—I'm happy you're not gone in a year. I would have hated to be the one to bring you that news.

Mr. PODONSKY. I think I need to be resuscitated.

Mr. COX. No, no. It's a problem of having things whispered to you from staff. The staff were just pointing out that the Secretary is going to be gone in a year, of course, or perhaps not, but we do have changes of administration and changes of personnel which leads to me what I hope will be a question that I will finally be permitted, and that is, whether or not any of the three of you can tell us that you are reasonably far along in narrowing a field of candidates for the new administrator of the NNSA? Is that something that you are taking responsibility for, any of you?

Mr. PODONSKY. No, sir.

Mr. COX. You haven't been asked for suggestions or to review credentials or qualifications of people?

Mr. HABIGER. No, sir.

Mr. COX. Well, I think that concerns me a little bit. Oughtn't you to be consulted on such a thing? Don't you have some expertise in those areas?

Mr. HABIGER. If I could, sir, not necessarily. The Department of Defense, as the commander-in-chief of one of our commands, I was asked to make inputs on people that work directly for me, but my colleagues at very high level, that was never an issue of discussion.

Mr. COX. All right. Well, I do certainly hope that this is progressing and that we don't have the Secretary acting as the administrator.

I thank the chairman.

Mr. UPTON. Thank you.

I have two additional questions, and I want to make an announcement, in conferring with my colleagues. We are going to—I'm going to ask—I have a couple of questions. Mr. Burr, who is in the next room, is going to ask another round of questions—I hope that's not a vote that I hear—and then we are going to adjourn. We will finish then with this panel, be finished, and we will start with Panel II at one o'clock.

Mr. Podonsky, at Sandia you found problems with access controls in areas where classified matter was used and stored. Can you give us just a couple of examples of that, help us with that?

Mr. PODONSKY. I am going to have to defer for a question in terms of whether I would get into classified or not.

Mr. UPTON. Maybe if you could just submit that for the record. And at this point, that gives me a good transition. All members will be able to ask and submit written questions, and they will stay in a classified state if you deem them to be, and we will put that in there.

The last question that I have before I yield to Mr. Burr, what troubles me as I look at these ratings, and you indicated that two were satisfactory, one was marginal. Marginal to me is not satisfactory. I guess by definition it's not.

I'd be interested to hear from each of the three of you with regard to what attention or what measures do you think we should

impose on the outside contractors when, in fact, that rating is not satisfactory, is—in other words, when it's not satisfactory or marginal? What additional pressures should we be able to see to bear on those when that happens, Mr. Curran?

Mr. CURRAN. Sir, I can only speak for our inspection process. If the inspection finds a CI program to be less than satisfactory, or even if it is satisfactory, there are recommendations we make to improve the system. If it's less than satisfactory, but they still have effective program, yet they're not where we would like them to be, we clearly state that, and we give them recommendations to fix it and fix it immediately. We will go back in 6 months to see if they fixed it. If they haven't, then we need to make changes. We don't keep going back. I mean, you either fix the problems—

Mr. UPTON. Can you provide—you know, one of the things I indicated my opening statement was the fact that we are going to be talking with Chairman Bliley about a bipartisan trip of members to visit a couple of these labs probably early next year. Would it be possible for us to see a list of the items—

Mr. CURRAN. Yes, absolutely.

Mr. UPTON. [continuing] by the labs in terms of what you found?

Mr. CURRAN. Some of these issues that we raised—for instance, in Livermore, we found it had a satisfactory program. There are issues that we say, you know, you need to do this better than you have been doing it, and there's other issues that they raised with us.

For instance, we need our people, our CI people at the laboratory to have access to security files, which they don't have at this point. General Habiger and I have been working on that, and that's going to be fixed. Our contractors, CI people at the labs, don't have a personnel list of people who are involved in high-risk programs. They need to know that for briefing, debriefing and whatever. We are going to fix that.

So not all the recommendations pertain particularly to lab. What we are looking for is to improve the overall DOE program as best we can.

Now, these items are coming out that need our attention that we have these Special Access Programs that are taking place in. The CI people are not aware of what those are. We need to fix those programs. But if a lab is less than satisfactory or marginal—if it is marginal, we may have to make changes right on the spot. If it is an effective program, but should be a lot better, then we will go back there and fix it. It is one shot. We don't just keep going back and back until we run out of narrative here.

Mr. PODONSKY. Mr. Chairman.

Mr. UPTON. Mr. Podonsky. Mr. PODONSKY. One of the things that we also look for—and there is a requirement as of August 31, 1999—after every one of our inspections, the facility, together with the PSOs, needs to provide us with a corrective action plan for comp measures and long-term corrective actions. And one thing that has never happened before in the Department is, security findings and issues do not always result in corrective action plans that got implemented.

Mr. UPTON. Does that corrective action plan include a time line in terms of when it is going to be fixed?

Mr. PODONSKY. Yes, sir, it is supposed to include that.

Mr. UPTON. That would be interesting for us to see before a visit to look, just since August 1999.

At this point I yield to the vice chairman, Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman. Let me follow up on where the chairman was, and that is with contractors because the contractors also go through an annual evaluation; and I think in hearings past, we have pointed out the discrepancies in what you found, Mr. Podonsky, as it related to their security status and, in fact, what the annual assessment of their job performance was. In some cases, at the end, it was satisfactory. You came with marginal or unsatisfactory, and at some point during the year, deficiencies were noted.

In June, Secretary Richardson issued a memo that said DOE is drafting a new contract clause that would place the labs' annual performance fee at risk.

General, what do you think about that proposal?

Mr. HABIGER. It is a great idea.

Mr. BURR. The contractors are not going to be too happy with that.

Mr. HABIGER. This gets back, sir, to the accountability issue, in terms of the contractors being accountable, as well as DOE employees being accountable.

We certainly got the University of California's attention. Sitting behind me as a spectator here is recently retired Air Force Colonel Terry Owens, who was in charge of security and counterintelligence for all of Europe. He is now the full-time Security Administrator for the University of California. Before, they had a part-time individual who came in 3 or 4 days a month.

Mr. BURR. General, out of all the things that you told me, that is one of the things that I hope is 100 percent accurate, because one question that I asked yesterday in our briefing was, did the University of California understand after their visit up here the seriousness with which we're going to take this issue. And I hope, in fact, that did get through to them and that your former colleague is not there just for window-dressing alone.

Mr. HABIGER. I guarantee you, sir, he is not. I know him well. He used to work for me.

Mr. BURR. Part of this requires a cultural change at the DOE because, in fact, when Mr. Podonsky goes into a facility, or Mr. Curran, when there is a suggestion from the security side of our inspection team that they had a deficiency, the contractor, as I understand it, cannot carry anything out until there is a policy directive from the Department of Energy.

You shake your head, General, but when there is a recommendation made—now, correct me if I am wrong, Mr. Podonsky—when there is a recommendation made, the Department of Energy has to then write the policy before the contractor—

Mr. PODONSKY. No, sir, first we don't make recommendations. We make findings and we issue findings that are tracked to see what the corrective action is going to be. Our findings are based on existing policy and performance.

I am not aware that the contractor does not take corrective action until there is a policy. It's—it's the lead PSOs that have the

responsibility to make sure that these things are being implemented and corrected.

Mr. BURR. Would I take for granted then that all the findings that you found are currently being acted on and that none of the findings are, in fact, idle?

Mr. PODONSKY. I wish that would be the case.

Mr. BURR. Then, of the findings that you have addressed, why is there not action on 100 percent of them?

Mr. PODONSKY. I would ask you to ask that of the PSOs and the laboratory, because what we tried—when we identify, it is a simple—

Mr. BURR. I think at the last hearing—I think you were in attendance when the University of California and other people, as well as the lab managers, testified, and I will look to our counsel in case I misunderstood it—my understanding was that their reasoning was that they didn't have the policy directive from the Department of Energy. I am told in certain cases, yes. I don't know that that gets us any further down this road. But what you're saying is that where you have had a finding, 100 percent of them haven't been acted on and that we need to ask the contractors and the labs why; is that correct?

Mr. PODONSKY. One hundred percent have not been acted on for various reasons. Some may, in fact, be resources. What we were talking about before, they may take compensatory measures, and we are looking for long-term fixes.

Mr. BURR. Did your team send to DOE management findings that DOE has not acted on?

Mr. PODONSKY. Yes.

Mr. BURR. And what percentage of your total findings would that be?

Mr. PODONSKY. It is a low percentage today, but part of that—and we understand the business of prioritizing those which are the priority ones, but I must hasten to say that what we have seen today in terms of response is a far better picture than what we've seen in past years.

Some of it is resource requirements, be it money or manpower; some of it is technology like in the cyber security arena. But I'm not—my point, that I'm trying to answer your question to, is it's not always, as far as we are concerned, tied to a policy shortcoming; there may be other variables there. But, to date, since the Secretary created this office in May of this year, most of the findings are being addressed, at least with compensatory measures.

Mr. BURR. Do we still have a policy of remote access to unclassified computers at the labs?

Mr. PODONSKY. I think General Habiger—

Mr. HABIGER. I addressed that while you were out of the room.

Mr. BURR. I apologize if I was out of the room.

Mr. HABIGER. No problem.

The problem was identified in August by Glenn. We have policy that will be out late next week that greatly tightens up that shortcoming, that his people identified, Glenn's people identified. They will make—if we're going to have people on that list of 25 countries that are sensitive and the terrorist countries that will have access to unclassified systems—

Mr. BURR. Is that a policy, then, that the contractor will administer?

Mr. HABIGER. You bet. And he will be accountable.

Mr. BURR. Tell me, was this not a road we were just down, a finding, a policy?

Mr. HABIGER. Well, let me, if I could, sir—and I think this is an important point because I got into this when I started getting smart about how the Department operates, legally, the contractor doesn't have to comply unless there is a policy. But I can tell you my relationships with the three national laboratory directors, and I have a very close working relationship with them; every time I've called them and talked to them about these kinds of issues, they've taken immediate action.

Mr. BURR. General, I hope that—I assure you that I will and I hope that you will go back and read the testimony of those individuals who testified in front of this subcommittee and how many times they said, we can't do it without the policy written by the Department of Energy. And I am sorry they're not here to testify as well.

Let me ask you, Mr. Podonsky, one last question. If we had a weapon stored at one of these facilities—and I think it is safe to say that we do—and somebody wanted access to that weapon, would they steal the weapon or would they steal the blueprint of the weapon, given that both had access that was as easy as the other?

Mr. PODONSKY. I think the way I would answer that is that we do not believe that nuclear material or weapons parts or components are at risk today. Our area that we are most concerned about is the information security. So, your hypothetical situation, I would say that they would be more attractive to go after the information as opposed to the actual material.

Mr. BURR. Thank you. I thank all three of you.

I yield back.

Mr. UPTON. Thank you.

Mr. Cox, do you have any further questions?

Mr. COX. Actually, Mr. Chairman, I have a number of questions, and I think if the panel would be willing to respond to the committee and follow up with written questions and answers we can handle most of them that way. There are a number of details that I think the committee ought to be very interested in, and so I would prefer to follow up that way on these details.

They are not just details. Many of the things—I think we could spend an hour talking about e-mail, because we are becalmed there. I know we are doing a lot to try to change the status quo, but in terms of results I think we're sort of where we started. And on and on.

There are a number of these issues that I think need to be covered. So if you are all willing, and if the committee is planning to do this in any case, I will pursue my questions through that route.

Mr. UPTON. We have indicated that we will, in fact, be pursuing that course.

Panel, thank you very much. We appreciate your time, your testimony, and we want very much to encourage your continued commitment to try and do your very best to make sure that all of these

secrets and facilities are, in fact, properly and adequately safeguarded.

Thank you very much. We will reconvene at 1 o'clock.

[Brief recess.]

Mr. UPTON. Okay. We are back. As you saw with the first panel, we have a long tradition of taking testimony under oath. Do any of you have objection to that?

We also, under both committee rules and House rules you are allowed to have counsel, do any of you wish or desire to have counsel?

If you would stand and raise your hands.

[Witnesses sworn.]

Mr. UPTON. Thank you very much.

We will start with Dr. Robinson.

TESTIMONY OF C. PAUL ROBINSON, PRESIDENT AND LABORATORIES DIRECTOR, SANDIA NATIONAL LABORATORIES; JOHN C. BROWNE, DIRECTOR, LOS ALAMOS NATIONAL LABORATORY; C. BRUCE TARTER, DIRECTOR, LAWRENCE LIVERMORE NATIONAL LABORATORY; GIL WEIGAND, DEPUTY ASSISTANT SECRETARY, STRATEGIC COMPUTING AND SIMULATION, U.S. DEPARTMENT OF ENERGY; AND JAMES TURNER, MANAGER, OAKLAND OPERATIONS OFFICE, U.S. DEPARTMENT OF ENERGY

Mr. ROBINSON. Thank you, Mr. Chairman. I think I, as well as all my colleagues, will try and be somewhat careful in our remarks today in an open session. In security matters, it is better to put any sensitive questions that involve vulnerabilities into a closed session—I don't know if that is possible—or else answer them for the record.

We also make a practice, which I think is also common sense, of not fully revealing the methods and practices that we put into use in monitoring because we get a bigger deterrent force by those.

Sandia has indeed had a long history of R&D responsibility for security technology, including the design of systems for nuclear weapons storage, for transportation and for site security. We have designed the site security for major military bases with high value as well as for airport security.

We have also become, over the years, specialists in cyber security. Thus, I take that our laboratory, as well as all the members of our staff, I believe, should have a higher obligation to be sensitive to security matters.

I would certainly like to clear up a problem in the last session where it was suggested that Sandia does not have security passwords for its computers. That was not the case. A very narrow question was raised in the I&E inspection about passwords, certainly not an across-the-board. Sandia has had a secure system of three levels of access for its computers since 1989, and a full fire-walled system between the restricted information and the open unclassified network. And we have always had a fully air-gapped system to our secure computers.

The sites that we operate do have distinct advantage, at least our New Mexico site, our site in Kauai, Hawaii and in Tonopah, Nevada. They are the equivalent of living in a gated community,

though perhaps a little stronger. They are fully contained within operating military bases. The principal site is completely within the site of Kirtland Air Force Base, and we carry out a close relationship with the security forces of our laboratory and the Air Force.

The DOE's independent oversight office in their inspection and evaluation in August of this year, in six of the areas, they declared "satisfactory," three areas they declared "marginal" with problems having been found in one area "unsatisfactory" and an overall of "marginal." I would point out that in prior years, in 1994, 1996 and 1997 and other DOE inspections of our security, we were satisfactory in all of those.

In 1998, a partial inspection had been done and we were marginal in a couple of areas there. I believe the review was, in fact, a useful review this time. And certainly a set of fresh eyes is always good to look at what's going on and spot something that you, operating every day, may not see, though I believe the biggest change is, in fact, that threats are changing and have changed over time. And we are not always as rapid to respond to those, and it is a good wakeup call when we do find something that does need to be fixed, and we have given high attention to fixing those.

We are trying to institute an approach to security that we found is successful in other areas, and I would call it applying quality methodologies in the security area. It is certainly not enough to try and inspect out all the defects in security. You have got to build the quality in as the foundation. That means getting every individual in the laboratory involved in their responsibility for security and put most of your emphasis there, which is what we do. We try to install an integrated security management system in a similar way to which we have done it in the environmental safety and health area with, I think, very high success.

I attached to my statement, which I assume you will accept for the record, a much longer statement, a comment about polygraphs. And, again, in the earlier session there was a statement that people hadn't been polygraphed. At our laboratory just under 200 people have been polygraphed, not as a result of a DOE directive but as part of other programs. The wish to extend polygraphs to a much wider area has caused me to have to look a lot more carefully at the underlying science of polygraphs if we are to, in fact, risk the future of the laboratory on this.

I attached as an appendix to my statement a report done by a number of my senior scientists which I commissioned to look at the underlying basis of polygraphs. I was not pleased with their findings. I don't think you will be either when you read as to the adequacy of polygraphs. If not applied carefully, we may in fact be making things less safe because when you crank down the polygraph to try and get a smaller and smaller number of false positives, you must at the same time open the doors to let real deceives get through. And in particular, when polygraphs such as these are to be used to apply—to allow someone to be given a clearance in advance of a background investigation, I think you are putting in a risk that I would find unacceptable.

Finally, let me say I think we've got to, in the future, put more attention on stopping the espionage problems in other routes than

just looking at security. I think attacking it directly. First of all, better background investigation—and I am pleased with the legislation that was just passed. I think our site will probably go up to exclusively Qs, which is how we used to operate throughout most of our history; and we will celebrate our 50th anniversary at end of this month.

I also believe it's appropriate with the level of security material and the responsibility we are given that sting operations are an approach to directly attack security problems, as well as greater surveillance activities of laboratory activities.

With that, I'll complete my oral statement.

[The prepared statement of C. Paul Robinson follows:]

PREPARED STATEMENT OF C. PAUL ROBINSON, DIRECTOR, SANDIA NATIONAL LABORATORIES

INTRODUCTION

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify today. I am Paul Robinson, director of Sandia National Laboratories.

Sandia National Laboratories is a multiprogram laboratory of the U.S. Department of Energy and one of three DOE laboratories with a research and development responsibility for nuclear weapons. Sandia's job is the design, development, and certification of nearly all of the non-nuclear subsystems of nuclear weapons. Our responsibilities include arming, fuzing, and firing systems; safety, security, and use-control systems; engineering support for production and dismantlement of nuclear weapons; and surveillance and support of weapons in stockpile. We perform substantial work in programs closely related to nuclear weapons, such as nuclear intelligence, nonproliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also performs research and development for DOE's energy offices, as well as work for other agencies when our unique capabilities can make significant contributions.

As you know, the DOE Office of Independent Oversight and Performance Assurance recently concluded a comprehensive inspection of safeguards and security at Sandia National Laboratories, New Mexico, and issued a report on August 23, 1999. The inspection gave "satisfactory" ratings in six topical areas in security at Sandia, "marginal" ratings in three areas, and an "unsatisfactory" in one area, resulting in an overall facility rating of "marginal." The security areas receiving "marginal" rankings were

- Unclassified Visits and Assignments by Foreign Nationals,
- Unclassified Cyber Security, and
- Protection Program Management.

The area receiving the "unsatisfactory" rating was Classified Matter Protection and Control. Our corrective action plan for addressing the findings and issues identified in the inspection is well under way.

A "marginal" facility rating is clearly unacceptable to Sandia, and we are committed to achieving a satisfactory evaluation at our next opportunity. However, I do not believe this score necessarily indicates that security has deteriorated at our site. Rather, I believe it reflects a new reality of higher threat levels than existed in the past and more rigorous requirements to counter them.

Because the inspectors' report is classified "SECRET," we cannot discuss its specific findings in open session. Consequently, I will give a general overview of Sandia's security programs and the initiatives that we are taking to improve performance. If the committee wishes to discuss the details of the inspectors' findings and our plan for corrective actions, I will be happy to provide information in closed session.

SANDIA IS COMMITTED TO EXCELLENCE IN SECURITY

The espionage threat against the DOE nuclear weapon laboratories is a matter of great concern to me and my colleagues at Los Alamos and Lawrence Livermore national laboratories and at the Department of Energy. We are all taking vigorous steps to address this threat in its various forms.

Sandia National Laboratories has always been managed by an industrial contractor. I believe our laboratory culture has been strongly influenced by its indus-

trial heritage, which began under the AT&T Bell Laboratories and continues today with Lockheed Martin. That heritage includes a strong cultural commitment to security. I am pleased but not surprised that the inspectors noted a positive and cooperative attitude among Sandia managers with whom they worked during the inspection. Sandians care!

In a programmatic sense, Sandia is one of the nation's top centers of expertise in security. For decades, Sandia National Laboratories has been a leader in security research for nuclear weapons, nuclear facilities, and nuclear materials. We have designed security systems for sensitive military installations and other facilities such as airports, for example. For more than thirty years, we have worked closely with the National Security Agency on nuclear control codes and hardware that implement the highest levels of code protection. We design and maintain the usecontrol systems (including the hardware, software, and code management subsystems) that ensure that the nation's nuclear weapons can be used only with proper authorization. We also design and develop the equipment, facilities, and information systems for secure transportation and storage of nuclear weapons. These systems are subjected to extensive testing to ensure that they are secure.

Sandia's design engineers and scientists associated with the nuclear weapons program and related national security programs have a deep appreciation of the gravity of their security responsibilities. And I can assure you that management at Sandia is equally serious about security. It is a fact, however, that the technological challenges of information security have grown enormously in recent years. It is a tougher problem than it used to be. The recent attention given to security at the DOE Defense Programs laboratories is salutary and will help us focus on the emerging challenges of security in the cyber age.

SECURITY AS A CONTRACTUAL OBLIGATION

Sandia National Laboratories is managed and operated by Sandia Corporation, a subsidiary of Lockheed Martin Corporation. As an officer of Sandia Corporation, I am well aware of my contractual responsibilities for security. Effective security is not a choice, it is a requirement. The management contract for Sandia National Laboratories is quite explicit in this regard:

The contractor shall conduct safeguards and security programs, including counterintelligence, physical security, protection of government property and information; classification and declassification of information and materials; safeguards of nuclear materials control and accountability; foreign national program; computer security; and personnel security and access control for laboratory staff and visitors.

Moreover, several DOE directives relating to security are incorporated by reference into the contract:

- DOE Order 470.1, "Safeguards and Security Program"
- DOE Order 471.1, "Identification and Protection of Unclassified Controlled Nuclear Information"
- DOE Order 471.2A, "Information Security Program and Manual for Classified Matter Protection and Control"
- DOE Order 472.1B, "Personnel Security Activities"
- DOE Order 474.1-2, "Nuclear Materials Management and Safeguards System Reporting and Data Submission"
- DOE Manual 475.1-1, "Identifying Classified Information"
- DOE Order 1240.2B, "Unclassified Visits and Assignments by Foreign Nationals"
- DOE Acquisition Regulation 952.204-70, "Classification/Declassification"

Sandia Corporation's prime contract with DOE is a performance-based contract. Performance under the contract is determined through a laboratory appraisal system. DOE evaluates Sandia's performance annually and issues the Sandia National Laboratories Multiprogram Laboratory Appraisal Report. This performance appraisal is based on a jointly negotiated appraisal agreement that defines specific performance objectives, performance measures, and performance expectations to be evaluated each fiscal year.

I and the directors of Sandia Corporation are mindful that unsatisfactory performance will impact our annual laboratory appraisal and reflect on the reputation and credibility of Lockheed Martin Corporation. Security performance is a part of each corporate officer's performance management plan. Thus, contractual motivations for satisfactory security performance exist, and they are tangible to management.

TRENDS IN SECURITY DURING THE 1990'S

Protection philosophies were clearly affected by the end of the Cold War. Concerns over espionage took a back seat to other worries, such as whether we could sustain

the program and the stockpile and whether we could get sufficient resources to do our work. There was a willingness to assume, perhaps, that the fall of the Soviet Union signaled the beginning of a new era of global peace in which espionage would not require the same level of concern.

The more relaxed attitude toward security was evident in certain policy changes. Secretary O'Leary ordered an aggressive declassification review program early in her tenure. In 1992 DOE relaxed the accountability requirements for controlled documents. The modified accountability program omitted requirements for unique document numbers and maintenance of accountability records for certain classes of documents, inventories, destruction certificates, written authorizations to reproduce, and internal receipting. DOE also eliminated the requirement that all personnel with access to limited areas have a Q clearance, encouraging instead the use of the less rigorous L clearance for employees without need-to-know.

The end of the Cold War also resulted in substantial budgetary reductions for the DOE laboratories. From fiscal year 1992 through 1995, the Defense Programs budget dropped 25 percent in constant dollars. In response to criticism by Congress and the Galvin Task Force (Secretary of Energy Advisory Board) that costs were too high, Secretary O'Leary pledged to reduce costs at the nuclear weapon laboratories by \$1.7 billion over five years beginning with fiscal year 1995. In response, Sandia committed to achieve \$250 million in cost reductions. The bulk of the savings came from reducing administrative support costs and overhead, such as processes for procurement and materials management, human resources, financial management, information systems, and facilities services including security. We reengineered our corporate processes to streamline these activities and achieve efficiencies comparable to those in private industry.

Meeting the cost reduction targets for security during this time was very challenging. Even so, Sandia's safeguards and security program continued to receive satisfactory ratings in external appraisals and assessments. We were complying with the applicable directives for DOE security programs. We didn't consider, however, that such compliance might not be a reliable indicator of actual performance. In my view, this was a logical flaw that lulled the DOE community into feeling good about security when it should have felt rather uneasy. Yes, we complied with the DOE directives without serious consideration as to whether our security programs were truly effective with respect to the evolving threats. As a result, our security capabilities remained static while the threats advanced.

In 1998 DOE and the laboratories both began to realize that their security capabilities had not kept pace with the evolution of security threats. A review by the DOE Albuquerque Operations Office that year, as well as our own internal assessment, identified areas where security capabilities and performance required improvement. We took immediate corrective actions (as we do whenever an inspection indicates vulnerabilities), we tried to identify root causes, and we formulated an action plan to develop long-term solutions to the issues. I am pleased that the recent comprehensive inspection of safeguards and security by the DOE Office of Independent Oversight and Performance Assurance found that Sandia made significant progress in correcting the deficiencies identified in last year's special survey. Nevertheless, our goal is not merely to correct items identified by inspections, but to improve and sustain the capabilities and performance of our security programs.

OVERVIEW OF SECURITY PROGRAM MANAGEMENT AT SANDIA NATIONAL LABORATORIES

We are implementing an approach to security management at Sandia that draws from a successful strategy DOE adopted a few years ago for managing environmental, safety, and health programs. Sandia's integrated safety management system (ISMS) is designed to enable safe and compliant mission work performance, rather than being focused on compliance alone. Integrated Safety Management is a DOE-wide program that Sandia helped develop and which we wholeheartedly support. The program has proved to be an effective and rational approach to sustaining excellence in safety performance over the long term. We are adopting a similar approach for security.

Sandia's Integrated Safeguards and Security Management System (ISSMS)

Sandia is in the process of implementing—with DOE's support and encouragement—an Integrated Safeguards and Security Management System (ISSMS) for all its security responsibilities. The first principle of security management under ISSMS is that line management is responsible for the protection of the assets entrusted to them: It is the realization by employees that security is not someone else's job, it is part of your own job. We can't just bring in security experts and give them the job; every single person bears responsibility.

ISSMS will establish clear and unambiguous lines of authority and responsibility for ensuring that secure operations are established and maintained at all organizational levels. It will ensure that personnel possess the experience, knowledge, skills, and abilities necessary to discharge their security responsibilities. And it will provide a way to allocate resources efficiently to address security and operational needs.

Our ISSMS methodology stresses the need to identify applicable security standards and requirements before work is performed. Administrative and engineering controls to prevent and mitigate security risks are tailored to the work being performed and designed into work processes. ISSMS will measure security performance in a way that will help us identify effective and ineffective practices. We will, of course, comply with all applicable DOE directives for security; but the ISSMS program will go beyond compliance to measure, evaluate, and improve actual security performance.

Funding for Internal Security Programs

Sandia National Laboratories and DOE spent about \$43 million on internal security programs at Sandia in fiscal year 1999. Of that total, \$37 million supported general safeguards and security programs, such as control and accountability of special nuclear materials, physical security systems, classified matter protection and control, protective force, and personnel security. Counterintelligence was funded at \$850,000 in FY1999; I expect the budget for counterintelligence (which is provided directly from DOE headquarters) to increase substantially in FY2000. Total funding for Sandia's internal security programs in FY2000 is expected to be nearly \$50 million.

Cyber security operations were funded at \$2 million in FY1999 and were increased by 30 percent in FY2000. In addition, we invested \$2.6 million for information security (InfoSec) improvements in FY1999 but discovered that much more is needed to meet the challenges revealed in the Cox Report. The Integrated Security Management Program of DOE's Office of Defense Programs calls for investments of approximately \$100 million per laboratory in FY2000 and about \$35 million per year in subsequent years for cyber security. That level of investment is far beyond what can be accommodated within the FY2000 budget.

Physical Security

Assets protection at Sandia encompasses a multitude of security interests ranging from government property to special nuclear materials. Naturally, with such a broad range of assets, there must be a graded approach to protection. The level of protection afforded a particular asset depends on the potential risk to national security, program continuity, and the health and safety of employees and the public. Sandia's security program is based on risk management, which in this context requires that higher risks get greater protection. This approach minimizes activities that add little protective value but increase program costs.

Physical security areas are established with appropriate levels of protection for the nature, sensitivity, or classification of protected material or information:

- Property Protection Areas are security areas established for the protection of unclassified DOE property against damage, destruction, or theft.
- Limited Areas are security areas defined by physical barriers used for the protection of classified matter or special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized persons. Exclusion Areas may be established within limited areas where mere presence in the area would result in access to classified matter.
- Protected Areas are established for the protection of special nuclear materials or vital equipment. Material Access Areas are contained within Protected Areas and have separately defined physical barriers constructed to provide sufficient delay time to impede or deter unauthorized access. Vital Areas are areas located within Protected Areas used for the protection of vital equipment.
- Restricted Access Areas are areas established to protect sensitive compartmented information facilities, central alarm stations, secondary alarm stations, secure communication centers, and automated information system centers.

Classified matter may not be stored or used in a facility until specific approval has been granted by DOE, based upon review and acceptance of the facility security plan and, if appropriate, an onsite survey. Control procedures are established to protect classified matter appropriately under all conditions: in use, storage, and transit.

Sandia's laboratory facilities in New Mexico, and its testing facilities in Nevada and Hawaii, are located on military installations, which provide significant additional security buffers. DOE limited areas are protected by physical barriers, access control systems, and alarm systems. Sandia's protective force patrols such areas

during nonstandard hours and has the capability to respond immediately to intrusion. In addition, the protective force at Sandia's major laboratory site on Kirtland Air Force Base, New Mexico, can coordinate with U.S. Air Force security police if necessary to respond to any major incident.

Personnel Security

The personnel security program at Sandia National Laboratories involves security clearances, security awareness and education, special personnel security assurance programs, and the foreign visits and assignments program. Personnel security is the keystone of an integrated security program. All functional areas of security depend on assuring that only people with the proper credentials have access to protected information and materials, and that those people are fully trained and equipped with the proper tools to carry out their security responsibilities.

Security Clearances—The first line of defense in personnel security is the requirement for security clearances. The vast majority of employees and resident contractors at Sandia National Laboratories today must obtain a U.S. government security clearance as a condition of employment. A DOE Q clearance is required of the subset of employees who may have a need to access nuclear weapon design information (secret and top secret restricted data). Most other employees must obtain the DOE L clearance, which is approximately equivalent to the DoD SECRET clearance. The DOE Q clearance requires a background investigation of the individual by an agency independent of DOE and a reinvestigation every five years. An L clearance requires only a national agency records check for violations of law or bad credit, and is repeated every ten years.

In addition to the requirement for a security clearance, the laboratories operate under the DOE policy of "need-to-know." This security principle requires that access to classified matter "be limited to persons who possess appropriate access authorization and who require such access (need-to-know) in the performance of official duties" (DOE Manual 471.2-1A, *Manual for Classified Matter Protection and Control*). A Q clearance alone does not provide access to nuclear weapons restricted data.

Until 1993, all employees and contractors were subject to a Q-level background investigation. In 1993, DOE changed that policy: The laboratories were urged to maximize the use of the less rigorous L clearances for employees whose job assignments did not require access to nuclear weapon restricted data. Consequently, thousands of individuals began to work and move about in the limited areas of the nuclear weapons laboratories without having been subject to the exhaustive background checks required for Q clearances.

I am pleased that the Defense Authorization Act for Fiscal Year 2000 requires Q clearance background investigations for all personnel who work in or around locations where restricted data is present. The law also empowers the Federal Bureau of Investigation to perform background investigations for special access programs and personnel security and assurance programs. These requirements should significantly strengthen personnel security at the laboratories.

Security Education and Awareness—The principle objective of the Security Education and Awareness Program is to ensure that employees, consultants, and subcontractors are equipped to protect sensitive and classified information, classified material, special nuclear material, and other government assets entrusted to them. An equal objective of this program is to motivate and instill a high level of security awareness in individuals concerning the protection of national security interests.

Four types of security briefings are conducted for our personnel. An initial security briefing is given to all new employees before they report to their job assignments. The purpose of this briefing is to inform both cleared and uncleared employees who will have access to security areas about their obligations to protect materials and information, and to educate them on local security procedures and access control requirements. A general facility overview is also given which familiarizes employees with their responsibilities in the protection of DOE interests.

A more comprehensive security briefing is provided to employees, consultants, and subcontractors prior to granting access to classified information. The purpose of the briefing is to inform individuals who have been granted a DOE security clearance of their security responsibilities when working with sensitive and classified information.

Annual security refresher briefings are required of all employees, consultants, and subcontractors possessing an active DOE clearance to reinforce information about security policy and responsibilities. The annual briefings are presented using a variety of delivery methods, including an on-line option, department meetings, or seminars and workshops.

A termination security briefing is given to all Sandia and contract employees when their security clearance is terminated, regardless of the reason. This briefing informs individuals of their continuing security responsibility.

On June 21 and 22, 1999, at the direction of Secretary of Energy Bill Richardson, Sandia (and the other DOE Defense Programs laboratories) suspended normal operations to conduct security immersion training for all employees. At Sandia, we reiterated long-standing DOE and laboratory security policies and briefed staff on the Secretary's zero-tolerance security policy. We placed special emphasis on the new implementations in cyber security. The laboratory's center directors were required to prepare training plans for those two days covering security topics appropriate for their work environments. Employees studied and discussed security policies and procedures, and many issues and suggestions were raised for follow-up. Frank discussions were held on the issue of the laboratory's culture and how it shapes attitudes toward security. In general, the two-day exercise was well received by our staff. Feedback indicates that it was an interesting, stimulating, and businesslike exercise.

I am aware that the House Committee on Science reported that 20 percent of the population of the DOE Defense Programs laboratories did not participate in the security stand-down training in June. That statistic is grossly inaccurate for Sandia National Laboratories. Ninety-three percent of our personnel completed the security stand-down training on June 21 and 22. Of the seven percent who did not participate on those dates, five of those percentage points were for people who were on previously scheduled vacations—not an unusual figure for late June (we insisted that employees not take vacation on those dates if they had not already scheduled it). Another one and one-half percent of the lab population were ill or excused for legitimate personal reasons. Less than one percent of the lab population were in work status on June 21 and 22 who did not take part in the security immersion activities. Some of those people were on business travel that could not reasonably be rescheduled. In addition, quite a few jobs—in our security and medical departments, for example—must be staffed at all times. However, all employees who missed security training during the stand-down have been required to make it up.

Foreign Visits and Assignments Program—To ensure compliance with DOE regulations, Sandia conducted a self-assessment of its foreign visits and assignments program prior to the recent safeguards and security audit. All the findings reported in this topical area by the DOE Office of Independent Oversight and Performance Assurance had been self-identified by Sandia. In addition, Sandia made several enhancements in its program in an effort to administer it more effectively:

- We increased the staff of the foreign visits and assignments program by 60 percent over the last year.
- We improved and expanded our education and awareness programs in their coverage of the requirements for foreign visits and assignments.
- We created a Foreign Interactions web page on Sandia's intranet, which is used as an information tool for the entire Sandia National Laboratories population and especially for Sandia hosts of foreign national visitors.
- Sandia's executive management formalized and published discipline guidelines as a mechanism for imposing consequences related to violations of foreign visits and assignments rules and regulations.

Nearly all of the foreign nationals who come to Sandia National Laboratories visit facilities that are outside the fence of the laboratories' limited (secure) area. Such facilities are called, in DOE jargon, "property protection areas" (PPAs). That terminology reflects the fact that no classified information or activities exist in those areas and that government property, rather than classified information, are the principal assets that require protection there. Ninety-eight percent of the uncleared foreign nationals who came to Sandia National Laboratories during 1998 visited property protection areas only. Nevertheless, we know that within that 98 percent, some visitors could be information-gatherers for their governments. For that reason, we brief Sandia employees on the risks and responsibilities of hosting foreign visitors. We require hosts to file a report after such visits to determine if any unusual activity occurred.

The two-day security immersion stand-down in June raised employee awareness of the policies and responsibilities with respect to hosting foreign national visitors or assignees. As a direct result of that exercise, several employees came forward to disclose previously unreported incidents during visits or assignments where security procedures had not been followed. We are reviewing those incidents to determine root causes and establish procedures to prevent recurrences. Security infractions may be assessed against some individuals if warranted.

We recently implemented additional measures to strengthen our controls over foreign visits and assignments:

- Sandia's foreign national program integrates key program elements (foreign interactions, counterintelligence, computer security, operational security, classification, and export control) in the approval process for foreign visits and assignments. The Foreign Interactions Office is the focal point for such visits and coordinates the reviews and approvals with the key program elements.
- Visits by uncleared foreign nationals must now be approved by a vice president of Sandia National Laboratories. The laboratory's executive vice president or president must approve visitors who are affiliated with sensitive countries. In addition, all visits and assignments from countries on the State Department's "Patterns of Global Terrorism 1998" list require prior approval by the Secretary of Energy. These countries are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.
- Sandia requires indices checks for all visits and assignments by foreign nationals who are citizens of or employed by a government or institution of a sensitive country, and for all visits and assignments requiring access to limited (secure) areas or involving sensitive unclassified subject matter. All indices checks are coordinated through Sandia's counterintelligence office. Any exception to this requirement must be approved by the laboratory director, and very few exceptions have been granted.
- Anytime a Sandia employee hosts a meeting or conference off-site where foreign nationals will be present (regardless of whether the meeting is held in Albuquerque, Livermore, or elsewhere in the world) the Sandia employee is responsible for going through the same formal approval process unless the event is open to the general public (per DOE Policy 142.1, the formal approval process does not apply to events open to the public).
- Foreign assignees (post-docs, limited-term employees, etc.) must be certified by the host as possessing unique technical skills not readily available to the laboratory from U.S. nationals.
- Foreign nationals visiting for longer than one day receive a red badge with photo and citizenship displayed.
- Badging of foreign nationals is centralized for consistency and better control.
- Foreign visitors and their hosts receive more extensive briefings on their responsibilities and obligations.
- A list of sensitive technologies recently developed by DOE is being used to help evaluate the appropriateness of visit access and topics.
- All foreign visit and assignment activity for Sandia is tracked on Sandia's own database systems. In July 1999, Sandia implemented the Foreign National Request (FNR) system to track foreign visits and assignments. The application can precisely identify, in real time, numbers of foreign nationals on-site, identities of foreign nationals and hosts, technologies, security restrictions, and statistical information used in managing foreign visit activity.

I must emphasize that foreign nationals are pervasive in the U.S. high-technology sector. Many of the top graduate schools in science and technology in the United States have majority populations of foreign students. U.S. companies have hired vast numbers of foreign nationals with technical degrees into their ranks. Forty-five percent of the visitors to Sandia National Laboratories who are affiliated with sensitive countries are from U.S. universities or U.S. companies. This exceeds even the number of visitors who represent their countries for official activities related to agreements in arms control, nonproliferation, and nuclear materials control (approximately 40 percent).

As you know, the FY2000 Defense Authorization Act imposes a moratorium on foreign visits and assignments to the DOE Defense Programs laboratories by citizens of sensitive countries. This requirement may prevent the laboratories from collaborating with U.S. universities or companies on some projects where citizens of sensitive countries are involved as students or faculty of universities, or as employees of U.S. companies. Consequently, we will work very hard to get our foreign visits and assignments program certified by the DOE Office of Counterintelligence, the Federal Bureau of Investigation, and the Central Intelligence Agency, as required by the law, as quickly as possible. We hope that those agencies will cooperate with us to perform that requirement expeditiously.

Cyber Security

Sandia has long been recognized as a leader in network security. Our three-level security structure, which has been in place since 1989 and fully deployed since 1995, has been adopted by DOE as a model for DOE laboratories and plants through the Tri-lab InfoSec Plan of April 1999. Sandia has stringent computer security procedures already in place, and we are improving our procedures based on our own re-

search and by adopting best practices from other DOE laboratories, industry, and other government agencies.

However, we recognize that policy, personnel training, and technology must continually be improved to meet the escalating threats. Recent attempts at espionage through cyber attacks highlight the necessity of very substantial action, and I appreciate the greater attention and support that cyber security is attracting. The Task Force for Integrated Security Management, referred to as "ISecM," is a joint endeavor of the three nuclear weapon laboratories and DOE, in consultation with DOE's production plants and field offices. The task force has recommended an ambitious program for a major enhancement of cyber security as a system of policy, people, and technology.

We have been working closely with DOE's chief information officer and the other Defense Programs laboratories to identify best practices. Three of these deserve special mention: The TAP utility, developed at Lawrence Livermore National Laboratory, supports the critical second layer of our three-layer process for monitoring email going to the unclassified internet for classified content. NADIR, developed by Los Alamos National Laboratory for monitoring usage patterns to detect suspicious behavior is another promising tool. StatePoint Plus software developed by Westinghouse is being implemented for security configuration management on our switched network. Cooperation among the laboratories and DOE has been excellent.

Sandia's classified network and computing environment has repeatedly earned high marks for security during numerous audits. Unfortunately, it has not earned high marks from the people who have to work in that environment for functionality and ease of use. We recognize that we must enhance the functionality of our classified multi-site network environment to allow secure, effective, and facile collaboration among the laboratories and DOE for classified work.

Sandia has aggressively implemented the action plan developed as part of the Tri-Lab Information Security (InfoSec) Nine-point Plan in April and the Secretary's Six Enhancements in June, 1999. We have completed 42 of the 46 actions called for in our InfoSec action plan. Two more actions will be complete before the end of the year. The remaining two are "red team" assessments that will be completed early next year, as soon as these scarce personnel resources are available.

Let me summarize some of the important actions we have completed as part of our InfoSec action plan:

- We have configured our unclassified restricted access networks at our sites in New Mexico and California so that electronic mail flows through a single control point. We are monitoring email messages to scan for classified content. So far, we have found that less than one in 10,000 of the email messages from high-risk areas of the laboratory are of concern, and those have been at the confidential level.
- We are strengthening the need-to-know controls over information on classified systems. For nuclear weapons data, we are improving the information infrastructure so that we can migrate from a set of physical islands of need-to-know groups to a more auditable and controllable need-to-know network. This new architecture will guarantee password protection, provide automated need-to-know controls, and record attempts to achieve access.
- We are reviewing and strengthening the need-to-know protection for sensitive unclassified information on our internal restricted-access networks.
- For authorized transfers of unclassified files from classified computers to unclassified computers, we are documenting approved transfer procedures that (1) require review of the material to be transferred by an authorized derivative classifier; (2) specify authorized transfer points and the required content for transfer logs; and (3) enforce two-person control by Qcleared personnel, one of whom must be current in the DOE Personnel Security Assurance Program (PSAP).
- We are exploring the feasibility of technical measures to prevent unauthorized transfers of classified files. We are also exploring the potential of individualized encryption codes for compartmentalized information.
- We are enhancing software protections on classified, secure email to provide redundant assurance that only the desired recipient has access to a classified message and attachment.
- We will perform red-team assessments of our unclassified and classified networks annually. Experts who are organizationally independent of the technical groups that design, maintain, or administer the networks will perform the assessments.
- We are monitoring all three levels (open, restricted unclassified, classified) to detect intrusion attempts and to respond decisively to those attempts.

- We have instituted a rigorous training program for our people who operate in the classified environment to ensure that they follow proper procedures in this quickly changing environment.

We are reviewing available U.S.-designed and built commercial products to augment the intrusion detection mechanisms on our networks. We employ user authentication, network intrusion, and vulnerability analysis software from industry, universities, and other government laboratories. Some years ago, Sandia implemented its own firewall between its open and restricted networks because we were not satisfied with any of the commercial firewall software available at that time. We recently identified a product from a domestic source that may provide a better firewall, and we are testing it for possible installation on our network.

The most popular commercial firewalls are produced by foreign owned companies. To mitigate the potential vulnerability of a nation-state attack through those foreign interests, we are working to validate and implement a commercial firewall from a U.S. vendor. A vendor has been selected and the firewall software has been acquired and installed in a test system. In hopes of meeting the December date for the next inspection, we are working through issues of reliability, vendor support, data-handling capacity, compatibility with our California site, and some apparent security anomalies that must be understood. We are committed to prudence even if the date for deployment has to be delayed.

We are pleased that our classified network received the satisfactory rating and our unclassified policies, networks, and personnel practices received favorable comments. However, we take seriously the overall rating of marginal for the unclassified system. The inspectors from the Office of Independent Oversight and Performance Assurance explained to us that the requirements for a rating of satisfactory have been tightened in response to the escalating threat. The standard is being raised faster than we have been able to respond. We are aggressively addressing the five action items from the audit to correct deficiencies. I must emphasize, however, that the recommendations of the Defense Programs' Task Force for Integrated Security Management (ISecM) must be funded and implemented in order to robustly address the escalating threat.

The cyber security threats encountered by DOE plague many agencies across the government, including the Department of Defense and the National Aeronautics and Space Administration. Unfortunately, the cyber security problem is very difficult and very complex. It is fruitless to attack this problem on a site-by-site basis; we need to address the problem in a systematic way for the complex as a whole.

The InfoSec Task Force recently published its report outlining an integrated system of policy, people, and technology for the nuclear weapon complex. In contrast to the current site-specific planning and accreditation that makes the system only as strong as its weakest link, the task force proposes integrated security at the system level for the nuclear weapons complex as a whole. Experts in computer science and communications from all three defense programs laboratories and the nuclear weapons production complex worked together to identify vulnerabilities and propose and implement countermeasures in the plan. According to their report, an investment on the order of \$100 million per DOE site and a continuing maintenance of approximately \$35 million per site to achieve very low levels of risk. Funds of that magnitude cannot be provided from existing programs and will require additional appropriation. The DOE Defense Programs Complex Information Security Action Plan is available from the DOE Office of Defense Programs.

Counterintelligence

We are building a counterintelligence program at the laboratory that responds to the President's direction in PDD-61 and implements DOE's Counterintelligence Implementation Plan. During 1998, Sandia's counterintelligence office actively contributed to the design of the DOE Counterintelligence Implementation Plan, which resulted in revamping the counterintelligence program at the laboratories. We moved Sandia's counterintelligence office out of the safeguards and security organization to a position with direct access to the laboratory director. We hired a 30-year veteran of the FBI to manage our counterintelligence program. The FBI is the lead agency with cognizance and expertise in all national counterintelligence and espionage matters, and it is appropriate that the laboratories' counterintelligence programs be staffed by individuals with that experience. Because of their professional "CI" background, they are knowledgeable of the FBI's investigative methodology. At the same time, because the counterintelligence personnel at the laboratories are part of the laboratory community, they are in a position to earn the trust and confidence of the scientists and engineers that is so important to the job.

Counterintelligence activities are now funded directly from DOE headquarters. The counterintelligence program at Sandia National Laboratories was funded at

\$850,000 in fiscal year 1999. We expect FY2000 funding to increase substantially. The higher level of funding will permit us to support four counterintelligence officers, a counterintelligence research analyst, one or more technical experts in cyber security, and additional support staff.

POLYGRAPH SCREENING

Many employees have expressed deep concern to Sandia's executive management and DOE about proposed polygraphy testing. In acknowledging the confusion and anxiety on this issue, I asked a group of Sandia's senior engineers and scientists for their thoughts and inputs. The seniors reviewed the literature on polygraphy and submitted a report summarizing expert opinion and expressing their own conclusions. Their report is attached as an appendix to this statement.

The report highlights several issues that as a laboratory director I find rather troubling:

- Many experts in the field of psychology believe that polygraphy is not theoretically sound and that claims of high validity for the procedure cannot be sustained. (This information was derived from a survey of members of the Society for Psychophysiological Research and Fellows of the American Psychological Association.)
- Studies performed by the Office of Technology Assessment and the Polygraphy Institute of the Department of Defense show that claims and estimates for the rate of false results in polygraph testing vary greatly.
- Reports by the Office of Technology Assessment, the Polygraphy Institute of the Department of Defense, and independent experts in polygraphy state that the effectiveness of polygraphs as a screening tool has not been established and appears to be much less than their utility for specific-incident investigations.
- The Office of Technology Assessment and independent authorities state that polygraph tests can be beaten through learned countermeasures.
(Reference citations for these issues are in the report.)

These issues raise serious concerns for those of us who bear responsibility for the long-term health and vitality of the laboratories and the success of the national security programs they serve. The Department of Energy must be very careful in how it designs and conducts its polygraphy program. If the program is mishandled, the resulting personnel problems could be very damaging to the laboratories and their national security programs.

Notwithstanding the safeguards and protections that DOE intends to incorporate into its regulations for the polygraphy program, significant issues remain for laboratory managers. One issue is the legitimacy and validity of the polygraphic process itself. Laboratory directors will have difficulty persuading their employees to embrace a screening methodology that they know is not generally accepted by the psychology profession, that many polygraphy experts regard as unreliable for screening applications, that is not amenable to objective measures of accuracy, that is prohibited by law in the private sector, and that can be fooled with learned countermeasures.

Thus, a major concern for the laboratories is what impact the polygraphy program will have on our retention of personnel in sensitive programs. Will those programs lose good people? Will they lose people with critical skills?

A related issue for laboratory directors is how the polygraphy requirement will affect recruitment. It has already become more difficult for us during the last several years to attract top graduates in engineering and science. We must already compete for those people with private corporations that can offer challenging technical work and more attractive packages of salary, benefits, stock options, and career advancement. If we will have to tell candidates that they may be subject to a scientifically questionable polygraph exam every few years, I am sure that many good people will be dissuaded from considering employment in the national laboratories. One study of polygraphy found that individuals with college degrees tend to have higher rates of false positives. My fear is that within ten to twenty years of a polygraphy program, we may not have the nation's best and brightest scientists and engineers looking after the reliability, safety, security, and control of nuclear weapons.

Finally, I am worried that excessive confidence in polygraphy may divert attention and resources from essential security programs that are more productive. We could put a lot of resources into a polygraph program for DOE and fail to aggressively improve the funding, staffing, and sophistication of our programs in cyber security, personnel security, security education and awareness, counterintelligence investigations, inter-agency coordination, and comprehensive periodic background re-

investigations. Polygraphy is probably the weakest tool in the security and counter-intelligence toolbox, and we should not cherish unrealistic expectations for it.

In view of the many uncertainties surrounding polygraphy, I believe DOE must proceed cautiously with a limited program that will be subject to reevaluation after an appropriate time.

CONCLUSION

The escalating security threat against the DOE nuclear weapon laboratories is a matter of great concern to me and my colleagues at Los Alamos, Lawrence Livermore, and the Department of Energy. The recent inspection of safeguards and security at Sandia National Laboratories by the DOE office of Independent Oversight and Performance Assurance was a useful independent review and provided me with insights that can only be seen with "fresh eyes." It helped identify several ways in which we can strengthen our security posture. We are taking vigorous steps to resolve all findings and issues identified by the inspection as quickly as possible. For the long term, we are implementing an Integrated Safeguards and Security Management System which will help us achieve excellence in security performance on a consistent basis.

The unmistakable message of the recent inspection is that security must stay ahead of the threats. The threats will always change as technology changes. Measures that were sufficient in the past no longer afford an adequate defense. Security policies and systems must be designed for capability and performance against real, current threats. Compliance is simply not enough.

Polygraphs and Security

**A Study by a Subpanel of Sandia's Senior
Scientists and Engineers**

October 21, 1999

Executive Summary

Because of concerns raised in Congress and the Executive Branch about inadequate security in the national nuclear weapons laboratories, the Department of Energy (DOE) plans to institute polygraph screening for some employees and applicants. These tests are intended to identify subversives and deter potential ones. This policy seemingly assumes that polygraph tests, test interpretation, and any follow-up processes will accurately identify subversives and nonsubversives. We conclude that there is no adequate scientific basis for this assumption. No specific polygraphic or behavioral response has been directly linked to the act of deception and there are too many subjective factors involved in the administration and interpretation of polygraph tests to be able to predict and control their effectiveness and limitations.

A review of the scientific literature on polygraph testing revealed substantial concern about polygraph accuracy for screening, and Federal law for most situations bars such usage. A summary of scientific opinion from a recent survey concludes that most psychology experts do not consider polygraphy to be technically sound and even more believe that skilled subversives can defeat polygraph tests.

Two general uses of polygraph testing are specific-incident investigations (as when an individual has been accused of a crime) and general screening (where a target population is tested to see if any of them have committed any crime). Published estimates of polygraph accuracy for specific-incident situations, based on the agreement of polygraph results with known facts, vary depending on the context in which data were obtained and the quality of data collection, selection, and analysis. A 90% accuracy rate is a reasonable expectation for adequately controlled specific-incident tests. It is, however, unwarranted to assume these accuracy rates apply to screening applications of polygraphy. Adequate studies have not been done for screening applications. Thus, it is impossible to predict what error rates (false negative—subversive passes polygraph test; false positive—innocent person fails polygraph test) and inconclusive results would occur in the proposed DOE screening. But, the costs and consequences of such errors need to be considered before the DOE policy is implemented. False positive results subject individuals to increased scrutiny and unwarranted suspicion. Even if a suspect is eventually exonerated, the process can damage that person's career and job performance. Such possibilities can make it more difficult to recruit and keep personnel with the high professional qualities on which the nuclear weapons program relies.

Issues resulting from false positive results have influenced agencies to "tune" polygraph tests (reduce the number of positive indications for screening). In fact the DOE has stated that a 2% positive indication is anticipated. Tuning polygraph tests to decrease positive results increases the probability of false negative results, thus reducing the intended effectiveness of the tool. Consequently, real subversives may be more likely to become insiders—particularly if over-reliance on polygraph testing leads to reduced emphasis on other security and counterintelligence methods.

Polygraph testing could drive away existing innocent, talented workers who have provided value to national security programs and deter prospective, talented employment candidates from considering a career in the national laboratories. Resources that could have been applied directly to national security programs or to finding more effective ways to enhance security may be wasted in administering a polygraph screening program and dealing with the consequences of false identifications.

We believe that the entire national laboratory security system should be improved using a systems approach in which the cost and benefits of changes can be plausibly estimated. A full systems evaluation is necessary because computer technology has fundamentally changed threats to national security. We doubt that polygraph screening of employees will provide value to an integrated security system.

Table of Contents

Preface	5
Charter.....	5
Acknowledgments.....	5
1.0 Introduction.....	6
2.0 Polygraphy.....	7
2.1 Theory.....	7
2.2 Applications.....	8
2.3 Accuracy.....	9
2.4 Countermeasures.....	11
2.5 False Results.....	13
2.6 Examiner Influence.....	15
3.0 DOE Implementation.....	17
3.1 Improvements Needed.....	18
4.0 National Security Concerns.....	19
5.0 Alternative Measures.....	20
6.0 Conclusions.....	22
Appendix I: Acronyms.....	23
Appendix II: References.....	23

Preface

Sandia's Senior Scientists and Engineers ("Seniors") provide a service to the Laboratories as independent, experienced, corporate evaluators of technical issues. They are available as a group to assist Sandia management with technical reviews of particularly significant issues and programs. Implementation uses subpanels of the Seniors (helped as necessary by other Sandia staff) to conduct the initial, detailed review of issues or programs. The reports of the subpanels are then made available for review by all other Seniors prior to submission to management.

This document is the report of the subpanel studying polygraphs and security at Sandia. Members of the subpanel are:

- Bob Benner, 9224
- Larry Bertholf, 4103
- Earl Boebert, 5901
- Dick Damerow, 2567
- Rob Easterling, 9800
- Lawrence Larsen, 15300
- Carl Melius, 8130
- Dana Powers, 6400
- Al Zelicoff, 5335

Charter

"I believe that the question of polygraphs is a central one that will occupy more and more of our time before it's over. ... The crux of the issue is that, while few if anyone really advocates the use of more extensive polygraphs as a screening tool (because of the false positive problems), a large body of opinion suggests that polygraphs are a useful investigatory tool. I confess to not knowing where we as a management team should stand on this issue ... I would appreciate your thoughts and inputs as to where we would like this issue to come out" C. Paul Robinson

Acknowledgments

Dianna Blair (9811) made major contributions to this report. Parts of the background, approach, text, references, and philosophy came from her. The Seniors on this subpanel are indebted to her and gratefully acknowledge her contributions. Jerry Allen (4100) encouraged us to consider alternatives to improve security. Dan Garber (4141) provided several editorial improvements. Julie Kesti (4915) provided literature searches and references. Larry Greher (11200) provided references to court cases, Bob Park (11300) helped us interpret the Employee Polygraph Protection Act, and Paul Shoemaker (5002) provided good "leads" and direction.

1.0 Introduction

Because of concerns raised in Congress and the Executive Branch about inadequate security at the national weapons laboratories, the Department of Energy (DOE)¹ plans to institute polygraph screening for employees who have access to the most sensitive categories of classified information and materials, as well as applicants for such positions. These tests are intended to identify actual subversives and deter potential ones. This policy seemingly assumes that polygraph tests, test interpretation, and any follow-up processes will accurately identify subversives and nonsubversives.

The best summary of polygraphy that we found is the Office of Technology Assessment (OTA) report. The OTA concluded that "while there is some evidence for the validity of polygraph testing as an adjunct to criminal investigations, there is very little research or scientific evidence to establish polygraph test validity in screening situations."^{2,3}

Although the accuracy of polygraph screening is very questionable, congressional legislation is mandating such screening by DOE: The proposed legislation requires a polygraph examination for all persons in "... positions with access to the most sensitive categories of classified information and materials, as well as applicants for such positions."⁴

Senator Domenici has made it clear that he is concerned about mandatory polygraph testing:

US Senator Pete Domenici today urged DOE Secretary Bill Richardson to carefully consider the implementation of mandatory polygraph tests for agency employees, contending that 'a polygraph cannot be the sole determinant of the fitness for duty of national security workers.'

'Loyal workers threatened by false positives must have rapid and sure recourse before their careers and work are ruined and critical national security programs are impacted through incorrect loss of key researchers,' Domenici wrote Richardson. 'Large numbers of such false positives may overload any system you devise to handle them. Complete plans to address this issue should be in place before large numbers of tests begin.'⁵

¹ Acronyms used in this report are given in Appendix I.

² *Scientific Validity of Polygraph Testing: A Research Review and Evaluation*, Office of Technology Assessment (Henceforth called the OTA Report), November 1983, p. 8. (available at <http://www.wws.princeton.edu/~ota/disk3/1983/8320.html>).

³ References are listed in Appendix II.

⁴ Polygraph Examination Regulation, *Federal Register*, v. 64, 45062 (1999) (to be codified at 10 C.F.R. pts. 709, 710, and 711) (proposed Aug. 18, 1999).

⁵ Pete Domenici, "Domenici Concerned Over Polygraph 'False Positives,'" Press Release, www.senate.gov/~domenici/press, August 6, 1999.

Senator Bingaman has expressed clear opposition to DOE's plans for implementing polygraphs:

I am writing to express my opposition to plans by the Department of Energy (DOE) for implementing counterintelligence polygraphs, as proposed in the Federal Register in August 18, 1999. This rule goes far beyond what I envision as being an appropriate use of polygraphs, which would be as a limited investigative tool in cases where other evidence suggests the possibility of espionage. My opposition is based on five factors.

1. The proposed rule's basic premise, that screening polygraphs offer a specially effective tool for detecting guilty individuals, is not supported by scientific evidence.
2. The provisions of the proposed rule are unacceptably vague on key issues, such as who would be subject to requirements of the rule, and overboard in the potential categories of individuals who might be affected.
3. The proposed rule, in my view, does not give sufficient consideration to the privacy and other legal issues that will result from DOE's proposed program.
4. The proposed rule takes what I believe to be an unrealistic view of the problem of false positives. I am concerned that persons who are judged to have "failed" a polygraph screening will not be easily cleared, as this would involve proving a negative. The latter will, in my opinion, be particularly difficult to do, judging from the partisan atmosphere in which DOE security issues have been treated over the last year.
5. As a result of the preceding four factors, I believe that the proposed counterintelligence polygraph program will make it much more difficult for the DOE laboratories to attract and retain the best and brightest scientific and technical talent.⁶

This report addresses an essential question: In a full systems context—as one of many security and counterintelligence tools—will polygraph testing add to or subtract value from the quality and security of the nuclear weapons program?

2.0 Polygraphy

2.1 Theory

We begin the discussion of polygraphy with information about the theory of polygraphy. The most commonly accepted theory underlying polygraph testing is that, when the person being examined fears detection, such fear produces a measurable physiological reaction (e.g., elevation of pulse, respiration, and blood pressure, and/or increased

⁶ Jeff Bingaman, "Proposed Department of Energy Polygraph Examination Regulation," Memo to Secretary Bill Richardson, September 16, 1999.

perspiration) if the person answers deceptively. Thus, in this theory, the polygraph instrument is measuring the fear of detection rather than deception *per se*. The examiner infers deception when the measured response to questions about a crime or an unauthorized activity is different than the response to other questions.

A very recent study by Eli Lehrer points out that basic polygraph technology has not changed in the last 60 to 70 years:

Skeptics and polygraph professionals agree that the fundamental technology, which measures breathing, pulse, blood pressure and galvanic skin response (sweating) has remained unchanged since ... the 1930s. American Polygraph Association President Richard Keifer says that computers have simplified the work but agrees that the measurements have not changed.⁷

The utility of the polygraph depends strongly on the subject's confidence that it detects deception. Subjects who have little technical training may be convinced that a polygraph can detect deception. On the other hand, national lab employees typically have graduate degrees in the physical sciences. The differences in mind set with respect to technology, the limitations of technology, and the resulting confidence in polygraphy are immense.

2.2 Applications

Two general applications of polygraph testing are specific-incident⁸ investigations (as when an individual has been accused of a crime) and general screening (where a target population is tested to see if any of them have committed any crime). Published estimates of polygraph accuracy for specific-incident situations, based on the agreement of polygraph results with known facts vary depending on the context in which data were obtained and the quality of data collection, selection, and analysis.

Polygraphs are used in conjunction with many test protocols—such as the Control Question Test (CQT), Guilt Knowledge Test, Relevant/Irrelevant Technique, and Peak of Tension Test. Polygraphs are used by experienced and new examiners in direct and in “blind” tests.⁹ They are also used when facts are known and tests are controlled and in cases when the “facts” are determined from confessions, evidence, and judicial decisions.

⁷ Eli Lehrer, “Lies, Damned Lies and Polygraph Tests,” *Insight on the News*, v. 14, n. 28, August 3, 1998, p. 44.

⁸ From page 98 of the OTA report: “A principal use of the polygraph test is as part of an investigation (usually conducted by law enforcement or private security officers) of a specific situation in which a criminal act has been alleged to have, or in fact has, taken place. This type of case is characterized by a prior investigation that both narrows the suspect list down to a very small number, and that develops significant information about the crime itself. When the polygraph is used in this context, the application is known as a specific-issue or specific-incident criminal investigation.”

⁹ In a blind polygraph test, the evaluator of the test uses only the information recorded during the test, has absolutely no interaction with the person being tested, and is assumed not to have any other information (such as demographic data) about the person tested.

In specific-incident applications with controlled conditions, polygraphy can be useful. The following psychology laboratory experiment is an example of conditions where reasonable accuracy may be achieved:

Prototypically, the experiment is a card test with one of 6 simple geometries on each card. The subject is shown one card, which one is unknown to the examiner. ... The polygraph examiner then shows each card to the subject and asks if this is the seen card. The subject replies 'no' after each trial. After repeated trials, the differential polygraphic response to the guilty knowledge (the seen card) can be detected about 90% of the time based on simple Autonomic Nervous System (ANS) reactions to the 'lie.'¹⁰

General screening applications of polygraphy are a totally different matter. The examinee is not naive; the screening accuracies are much lower; and there is much more at stake than a card experiment (such as national security, clearances, jobs, and jail). Furthermore, measures to counter the effects monitored by the polygraph have been found and the use of countermeasures by a guilty party upsets the conditional probabilities of accurate detection and identification.

For both specific-incident and screening applications, many external variables can influence test results, including countermeasures, test protocol, test calibration, and the personalities, biases, and tactics of the interrogator and the subject. A summary of scientific opinion from a recent survey concludes that most psychology experts do not consider polygraphy to be technically sound and even more believe that skilled subversives can defeat polygraph tests.¹¹

2.3 Accuracy

What is the accuracy of a polygraph? One might as well ask, "What is the accuracy of a computer, pencil, or automobile?" It depends on what it is used for, how it is administered, and who is using it.

A summary of more than 2000 specific-incident cases in the 1980s shows an accuracy of 98% for cases where the examiner was directly (or interactively) involved in the decisions. In more than 900 specific-incident cases during the same time period, the accuracy was 90% for evaluators performing blind tests.¹²

In 1983, the OTA provided the following summary of results for research on the CQT in specific-incident criminal investigations:

¹⁰ Dawson et al., "The Electrodermal Response," *Principles of Psychophysiology—physical, social and inferential elements*, J. T. Cacioppo and L. G. Tassinari, Eds., 1990, p. 312.

¹¹ W. G. Iacono and D. T. Lykken, *J. App. Psych.*, v. 82, 1997, pp. 426-433.

¹² Norman Ansley, "The Validity and Reliability of Polygraph Decisions in Real Cases," *Polygraph*, v.19, 1990, pp. 169-181.

- Six previous reviews of field studies: average accuracy ranged from 64 to 98 percent.
- Ten individual field studies: correct guilty detections ranged from 70.6 to 98.6 percent and averaged 86.3 percent; correct innocent detections ranged from 2.5 to 94.1 percent and averaged 76 percent; false positive rate (innocent persons found deceptive) ranged from 0 to 75 percent and averaged 19.1 percent; and false negative rate (guilty persons found nondeceptive) ranged from 0 to 29.4 percent and averaged 10.2 percent.
- Fourteen individual analog studies: correct guilty detections ranged from 35.4 to 100 percent and averaged 63.7 percent; correct innocent detections ranged from 32 to 91 percent and averaged 57.9 percent; false positives ranged from 2 to 50.7 percent and averaged 14.1 percent; and false negatives ranged from 0 to 28.7 percent and averaged 10.4 percent.¹³

What, then, is meant by polygraph accuracy? The short answer is that in many studies on polygraphy, accuracy “refers to the number of correct decisions of the total number of decisions, after the inconclusives have been set aside [emphasis added].”¹⁴ In general, accuracy is a weighted average of the percentages of true positives and true negatives. These averages are questionable because of differing test conditions.

The OTA report also comments on polygraph accuracy:

A major reason why scientific debate over polygraph validity yields conflicting conclusions is that the validity of such a complex procedure is very difficult to assess and may vary widely from one application to another. The accuracy obtained in one situation or research study may not generalize to different situations or to different types of persons being tested.¹⁵

A great deal of information highlights the gulf between polygraph accuracies for specific-incident cases and for screening. Illustrative information is summarized below.

The OTA report expresses reservations about use of the polygraph for screening:

... while there is some evidence for the validity of polygraph testing as an adjunct to criminal investigations, there is very little research or scientific evidence to establish polygraph test validity in screening situations, whether they be preemployment, preclearance, periodic or aperiodic, random, or dragnet [emphasis added].¹⁶

D. T. Lykken recently reported similar concerns about polygraph screening tests:

Concerned by the lack of evidence for the validity of these procedures, the Subcommittee [US House Select Committee on Intelligence in 1979] urged the director of the Central Intelligence Agency (CIA) to institute research on the

¹³ OTA Report, p. 97.

¹⁴ N. Ansley and M. Garwood, *The Accuracy and Utility of Polygraph Testing*, US Department of Defense Report, Washington, DC, 1984, p.61.

¹⁵ OTA Report, pp. 7-8.

¹⁶ OTA Report, p. 8.

'accuracy of the polygraph in the pre-employment setting and to establish some level of confidence in the use of that technique.' No credible research on the important topic, however, has as yet been published. ... No one knows whether the screening test has some, slight, or no validity at all.¹⁷

According to a Department of Defense Polygraph Institute report about the use of polygraphs for screening in a controlled test with programmed guilty or deceptive examinees, accuracies ranged from 55.6% to 83.3%.¹⁸ The 55.6% number is not much better than chance, especially since the inconclusive decisions were excluded.

Clearly the use of polygraph testing for screening is problematic. We return to the OTA report for a concluding statement about polygraph accuracy in general:

No overall measure or single, simple judgment of polygraph testing validity can be established based on available scientific evidence [emphasis added].¹⁹ There are two major reasons why an overall measure of validity is not possible. First, the polygraph test is, in reality, a very complex process that is much more than the instrument. Although the instrument is essentially the same for all applications, the types of individuals tested, training of the examiner, purpose of the test, and types of questions asked, among other factors, can differ substantially. ... For example, there are differences between the testing procedures used in criminal investigations and those used in personnel security screening. Second, the research on polygraph validity varies widely in terms of not only results, but also in the quality of research design and methodology. Thus, conclusions about scientific validity can be made only in the context of specific applications and even then must be tempered by the limitations of available research evidence.²⁰

2.4 Countermeasures

The fact that countermeasures can affect the results of a polygraph test is well established. For instance, the OTA report has the following comments on countermeasures:

Theoretically, polygraph testing—whether for personnel security screening or specific-incident investigations—is open to a large number of countermeasures, including physical movement or pressure, drugs, hypnosis, biofeedback, and prior experience in passing an exam [emphasis added]. The research on countermeasures has been limited and the results—while conflicting—suggest that validity may be affected. OTA concluded that this is particularly significant to the extent that the polygraph is used and relied on for national security purposes, since even a small

¹⁷ D. T. Lykken, *A Tremor in the Blood*, Plenum Press, NY, 1998, p. 161.

¹⁸ *Comparison of Psychophysiological Detection of Deception Accuracy Rates Obtained Using the Counterintelligence Scope Polygraph and the Test for Espionage and Sabotage Question Formats*, Department of Defense, Fort McClellan, AL, Polygraph Inst. Report No.: DODPI93-P-0044; DODPI-R-0008, June, 95, Abstract.

¹⁹ OTA Report, p. 4.

²⁰ OTA Report, p. 4.

false negative rate (guilty person tested as nondeceptive) could have very serious consequences [emphasis added].²¹

If polygraph testing is to be more widely employed in national security investigations, there is an urgent need for research on countermeasures. Particular priorities would be research on drugs, biofeedback training, and subject gullibility, and motivation. Such research needs to be carried out both in field situations and in the laboratory. There are a number of drugs that are suspected of lowering ANS arousal and that theoretically may be able to invalidate the results of a polygraph examination or compel an 'inconclusive' finding. A first priority is to extend ... research on meprobamate (which reduced detectability) to other psychoactive drugs. Biofeedback training, as well as other forms of training have not been investigated, yet their effects on polygraph examinations may be substantial. Subjects' beliefs about the accuracy of the polygraph may also be critical. As suggested by the research ... individuals who believe their underlying thoughts are detectable are more likely to provide truthful responses. The reverse phenomenon seems feasible and it would seem possible to train individuals to believe that the polygraph is ineffective. Such training might be accomplished by providing individuals with false feedback on the polygraph as well as by specific instructions during simulated polygraph examinations. Similarly, subjects who can be easily trained to beat the polygraph may be more desirable as intelligence agents [emphasis added].²²

Similar comments appear in the *Journal of Applied Psychology*:

Effects of countermeasures on the CQT polygraph test were examined in an experiment with 120 subjects recruited from the general community. Subjects were given polygraph tests by an examiner who used field techniques. Twenty subjects were innocent, and of the 100 guilty subjects, 80 were trained in the use of either a physical countermeasure (biting the tongue or pressing the toes to the floor) or a mental countermeasure (counting backward by 7) to be applied while control questions were being presented during their examinations. The mental and physical countermeasures were equally effective: Each enabled approximately 50% of the subjects to defeat the polygraph test. ... Moreover, the countermeasures were difficult to detect either instrumentally or through observation.²³

A summation of the professional view of polygraphy is found in a recent article in the *Journal of Applied Psychology*. "92% of a scientific psychology community believes criminals or subversives can beat a polygraph."²⁴ That is, countermeasures, or methods to defeat detection, are believed to be effective by the knowledgeable scientific community.

²¹ OTA Report, p. 5.

²² OTA Report, p. 91.

²³ C. R. Honts, D. C. Raskin, and J. C. Kircher, "Mental and Physical Countermeasures Reduce the Accuracy of Polygraph Tests," *J. Appl. Psych.*, v. 79, n. 2, 1994, pp. 252-259.

²⁴ W. G. Iacono and D. T. Lykken, *J. App. Psych.*, v. 82, 1997, pp. 426-433.

A 1999 article by Robert Park presents a similar opinion from a Federal Bureau of Investigation (FBI) expert:

'There is almost universal agreement that polygraph screening is completely invalid,' Federal Bureau of Investigation polygraph expert Dr. Drew Richardson asserts. (Richardson taught his 10-year-old son to beat the test.) In 1997 Senate testimony, Richardson warned, 'To the extent that we place any confidence in the results of polygraph screening, and as a consequence shortchange traditional security vetting techniques, I think our national security is severely jeopardized.'²⁵

The DOE Polygraph Examination Regulation states that "A counterintelligence-scope polygraph examination both serves as a means to deter unauthorized disclosures of classified information and provides a means for possible early detection of disclosures to enable DOE to take steps promptly to prevent further harm to the national security."²⁶ If polygraph countermeasures are as effective as indicated above, it seems unlikely to us that polygraph examinations will be effective in either deterring or detecting "unauthorized disclosures."

2.5 False Results

The fact is well established that polygraph tests produce false results, especially tests used for screening. This section details the magnitude of the problem and notes the bias against innocent, loyal employees. Unfortunately, the solution to the false positive problem is not apparent. The Seniors believe that preventing this problem (by not mandating polygraph testing) is much more appropriate than trying to find cures *ex post facto*.

False negatives. False negative results (subversives who "pass" the polygraph test) pose an obvious increased threat to national security. This major issue seems to have been overlooked by the public, their elected representatives, and the rest of the bureaucracy.

James Matte comments on false negatives:

Perhaps the greatest danger is that a clever and convincing psychopath can talk a polygraph examiner into believing him even though the polygraph charts indicate deception.²⁷

The failure of a set of polygraphs to expose Aldrich Ames is particularly revealing. There are several possible reasons why Ames may have been able to defeat polygraph

²⁵ Robert L. Park, *What's New*, Washington, DC, Jun. 25, 1999.

²⁶ Polygraph Examination Regulation, *Federal Register*, v. 64, 45062 (1999) (to be codified at 10 C.F.R. pts. 709, 710, and 711) (proposed Aug. 18, 1999).

²⁷ James Matte, *Forensic Psychophysiology Using the Polygraph*, J.A.M. Publications, 1996, p. 296.

tests. He may have used one or more countermeasures,²⁸ he may have taken so many tests that he had no confidence in the polygraph, or perhaps the false positive rate was artificially reduced to the point that real positives were minimized. David Wise focuses on the examiners:

The problem ... was that the examiners in each case had failed to establish the proper psychological atmosphere of fear and intimidation. Unless the subject is afraid of detection the experts said, the needle won't jump. The tests ... were invalid because the examiners were too friendly.²⁹

In a screening application, the polygraph cannot identify a false negative. Thus, the weapons laboratories must use an individual's subsequent actions (as in the Ames case) to infer that a polygraph test provided a false negative. Clearly, the percentage of the work force that "passes" a polygraph-screening test via false negatives cannot be determined. To the degree that any credence is placed in polygraph tests, this is yet another argument against using polygraphs for screening.

False positives. In 1983, the OTA concluded "that the mathematical chance of incorrect identification of innocent persons as deceptive (false positives) is highest when the polygraph is used for screening purposes [emphasis added]. The reason is that, in screening situations, there is usually only a very small percentage of the group being screened that might be guilty."³⁰

The fact that false positives are widely known to be a problem is illustrated by part of the proposed legislation: "The Secretary shall prescribe any regulations necessary to carry out this section. Such regulations shall include procedures, to be developed in consultation with the Director of the Federal Bureau of Investigation, for identifying and addressing 'false positive' results of polygraph examinations."³¹

The following decision tree illustrates the problems with false results. It starts with 5000 employees being tested where 1% (50 persons) are assumed to be subversives (S) and the remaining 99% (4950 persons) are assumed to be not subversive (S*). This tree shows that even when a very generous accuracy of 90% is assumed for this screening application, 91.7% of those charged as guilty by the "lie detector" are, in fact, innocent. This represents a bias against the innocent of more than 10 to 1.

²⁸ The KGB told Ames, "Get a real good night's sleep. Be fresh and rested. Be cooperative. Develop rapport with examiner. ... And try to remain as calm and easy as you can." (See David Wise, *Nightmover*, Harper Collins, 1995, p. 146.)

²⁹ David Wise, *Nightmover*, Harper Collins, 1995, p. 211.

³⁰ OTA Report, pp. 5-6.

³¹ National Defense Authorization Act for Fiscal Year 2000 (Printed w/ House Amend.), S. 1059, 106th Cong. § 3187(d) (1999).

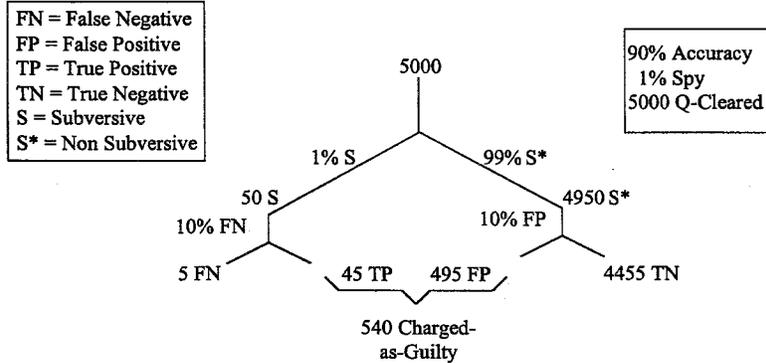


Figure 1. Polygraph Predictions.

Because it is impossible to prove a negative, using such techniques to determine an employee's suitability puts the employee at a great disadvantage. Raising doubts about a person's loyalty or security performance can adversely impact that person's career. With reported polygraph screening accuracy rates, 10% to 50% of national laboratory employees interrogated might be labeled security risks. Furthermore, relying heavily upon such a technique would result in a false sense of security. As discussed in Section 2.4, subversives can learn countermeasures to evade detection.

2.6 Examiner Influence

A subtle but significant part of polygraphy is the reliability of the polygraph examiner. All humans (even polygraph examiners) have biases of one sort or another that can create errors in polygraph test interpretations.

The accuracy of polygraph tests for screening is poor even with examiners who were probably unbiased. The large-scale implementation of polygraph screening at the weapons laboratories will require hiring many more examiners. Yet to prove that examiners are fair, DOE will have to construct tests to winnow the list of examiners (including current ones). Given that people who discriminate tend to believe in their actions, what kind of tests should be used? The ability to come up with a list of qualified examiners who can also create impartial fear and intimidation is a daunting task.

Examples. Examiners may influence polygraph tests in a number of ways.

According to Norman Ansley, the difference between direct and blind polygraph tests can affect accuracy (See Section 2.3):

A summary of more than 2000 specific-incident cases in the 1980s shows an accuracy of 98% for direct examiner decisions. In more than 900 specific-incident cases during the same time period, the accuracy was 90% for evaluators performing blind tests.³²

An article in the *Journal of Applied Psychology* makes the point that experts perceive examiners and tactics as important factors in polygraph tests:

When experts were asked if they would they submit to a 'friendly' polygraph (e.g., one administered by their lawyer), if they were guilty of a crime, 73% responded in the affirmative. However, only 35% would agree to take an 'adversarial' polygraph (say one administered by a prosecutor), if they were innocent.³³

James Matte discusses the potential vulnerabilities of examiners to con artists:

Perhaps the greatest danger is that a clever and convincing psychopath can talk a polygraph examiner into believing him even though the polygraph charts indicate deception.³⁴

In this last instance (which includes the Aldrich Ames case discussed in Section 2.5), polygraphs are worse than useless—they are a significant threat to national security.

This issue subsumes the issue of examiner certification. Certification is necessary but may not be sufficient. Ames' examiner was certified, the examiners involved in CIA sex discrimination cases³⁵ were certified, and it seems reasonable to assume that the examiners involved in the accuracy studies given in the first example were certified. Yet, in all these cases, examiner influence is clear.

Who will guard the guardians? We recognize that DOE will use controls to reduce examiner influence. However, we believe that additional actions may be necessary. DOE needs to ensure that examiners do not place any individual at a disadvantage for extrinsic reasons. This can happen during the pre-interview, the test, or re-examinations. DOE needs to determine whether the procedure is more threatening to particular ethnic groups, age groups, or genders. We believe that statistics should be kept and made available to the public regarding all non-negative results (deception indicated, no opinion, refusal to be tested, and test termination). Also, demographic and other pertinent information on all examiners should be a matter of public record.

³² Norman Ansley, "The Validity and Reliability of Polygraph Decisions in Real Cases," *Polygraph*, v.19, 1990, pp. 169-181.

³³ W. G. Iacono and D. T. Lykken, *J. App. Psych.*, v. 82, 1997, pp. 426-433.

³⁴ James Matte, *Forensic Psychophysiology Using the Polygraph*, J.A.M. Publications, 1996, p. 296.

³⁵ Daniel Jeffreys, "Getting Down on 'The Farm.' (CIA's humiliating polygraph tests are making it difficult to hire and keep operatives: reprinted from *The Independent*, Nov. 27, 1996)," *World Press Review*, v. 44, n. 3, March, 1997, p. 30.

Other agencies are being sued because of alleged abuse and discrimination. DOE should minimize potential diversion of national security funds to litigation and should demonstrate a commitment to diversity. Although the above measures may help, we believe that the best way for DOE to do this is to refrain from polygraph screening tests.

3.0 DOE Implementation

The following flow diagram is a draft description of how we think DOE will implement the newly proposed polygraph process.³⁶

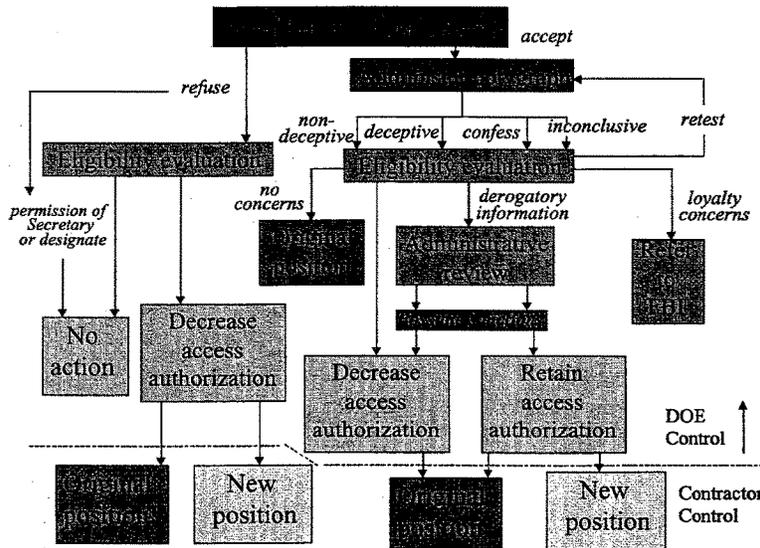


Figure 2. Draft flow diagram for the DOE polygraph process.

DOE plans to reduce the number of positives to reduce the issues resulting from false positives. The "Catch 22" is the minimization of real positives and the increased risk that subversives will not be detected. Reducing the target number of positives to an arbitrarily low number (2% is the security czar's suggested number) will almost ensure

³⁶ This description was derived based on a draft version of DOE N 472.2 "Use of Polygraph Examinations," a memo from Vic Reis to Rose Gottemoeller (Subject: Issuance of Notice on Use of Polygraph Examinations) with attached comments dated March 11, 1999, conversations with Richard Brown DOE/Defense Programs, and a DOE draft policy from the Office of Counterintelligence, 10 CFR part 709, Polygraph Examination Regulations.

that some guilty people will pass. Further, by giving individuals accused of wrongdoing the opportunity to exonerate themselves by taking a polygraph and by speeding up clearance processing by offering applicants a polygraph (now permitted), ill-intentioned people may more easily remain or become workers in the weapons complex.

Although scientific debate continues on the accuracy of polygraph techniques for ascertaining past criminal activities, the validity of using polygraphy for screening employees to predict future behavior is very questionable.

3.1 Improvements Needed

The Seniors do not trust polygraph testing to screen employees. Nevertheless, we recognize that polygraph tests may still be imposed by Congress and the DOE. If polygraph screening is required, the following suggestions and questions must be addressed.

DOE must act to minimize the undesirable side effects of polygraph screening. The most immediate side effect is that of low morale and possible inconclusive and false positive responses. The announced policy of transferring people from a "cleared" job to an "uncleared" one is not enough—there are issues of records and career progression and development within the laboratories. In the longer term, DOE will have to refine its internal security systems to detect individuals who can deceive the polygraph. DOE will also have to address the issue of polygraphs in recruiting. How can negative recruiting effects be mitigated when a potential recruit is told that such testing may be required for employment?

Will those who are already employed and cleared have their access withdrawn until their evaluations are complete? Who will make career-impacting decisions and on the basis of what additional information? Will a standard background reinvestigation suffice or will a more thorough one be initiated? Will DOE focus its finite resources on individuals who probably pose no threat to national security instead of on effective systems to eliminate subversives? During the polygraph process, examinees will provide a great deal of information from both control and security-related questions. How will this information be used? Should individuals have the right to receive a copy of their polygraph results? What will the DOE's policy be for passes, fails, and inconclusives?

DOE should establish a much clearer process regarding polygraphs. The process should include:

- a clarification of employees eligible for polygraph testing (Positions that DOE has determined have "access to the most sensitive categories of classified information and materials, as well as applicants for such positions" is too broad.),
- a clear indication of the types of behavior that are being searched for in the testing,

- a clear indication of the process to be followed once a positive or inconclusive indication is found or if the use of deliberate or inadvertent countermeasures is suspected or detected,
- the right of appeal and what constitutes an acceptable defense against an accusation,
- an indication of the documentation that will accompany an accusation,
- some proof that the follow-up will not bear any resemblance to anecdotal accounts of past practices for reviewing security suitability of employees accused in other venues (Note that in Figure 2, the far right hand side—referring loyalty concerns to the FBI—raises the specter of McCarthyism.), and
- a definition of the exceptions and an explanation about why should they be allowed (In Section 709.25 the DOE reserves the right under “a limited national defense and security exception” to rely on the results of a polygraph as the sole basis for taking action.).

Private sector employees are protected from blanket use of the polygraph by the Employee Polygraph Protection Act of 1988 (EPPA), which stipulates that an employer can be fined \$10,000 for even suggesting that an employee take a polygraph as a condition of employment. Unfortunately, the EPPA excludes individuals working in national security from this protection. An executive order protects federal employees from repercussions if they refuse to take a polygraph; placement of this information in the employee’s personnel file is forbidden. However, similar protection of national laboratory employees has not been adjudicated—they may or may not be protected.

What happens to national laboratory employees who refuse to be polygraphed? Supposedly, they will be moved to positions of equal responsibility and opportunity that do not require a access to sensitive information. However, finding an equivalent position may be impossible because of the specialized nature of work at nuclear weapons laboratories. Thus, it is possible that refusing to be polygraphed will result in career impacting consequences.

4.0 National Security Concerns

Potential impacts of false positives on national security are that (1) talented and loyal individuals may either leave or never seek employment at the laboratories and (2) resources may be wasted to clear the falsely accused and settle lawsuits.

Polygraphy testing will impact recruiting and retention. Some persons may “fail” the test and others may refuse on principle to take the test because of the polygraph’s demonstrated lack of validity. In the long term, this will erode the caliber of the laboratory’s technical staff, with obvious impacts on research and development.

In the short term, employee commitment and morale may be lowered because polygraph screening tests create an atmosphere of distrust between employer and employee, are

demonstrably unreliable, and indicate that DOE is unwilling to base security concerns on evidence. Daniel Jeffreys quotes some cogent words of warning on this subject: “‘The polygraph test is undermining morale throughout the [CIA],’ says Michael Kelly, a former intelligence officer who is now an attorney specializing in employee lawsuits against the CIA.”³⁷

A recent survey of Sandia National Laboratories employees has indicated similar concerns regarding morale, recruiting, and retention:

With respect to external recruiting ... an estimated 27% of the technical staff would not have applied to Sandia if a polygraph examination had been required.

With respect to retention, a total of 32% would (9%) or might (23%) transfer out of a position that required a polygraph and 15% would (2%) or might (13%) resign from Sandia if a polygraph was required.

[T]he effect on morale is another concern with respect to staff quality and productivity. Overwhelmingly ... the respondents anticipate a negative effect ... About one-half anticipate a somewhat negative effect and another one-third anticipate a very negative effect, in contrast to the 3% that anticipate a positive effect.³⁸

The Seniors believe that a threat to the national laboratories’ mission readiness has a basis in reduced congressional trust of DOE and the laboratories. This lack of trust is evinced in a bill recently passed by the US Senate: “The Secretary may not permit a covered person to have any access to any high-risk program or information unless that person first [emphasis added] undergoes a counterintelligence polygraph examination and consents in a signed writing to the counterintelligence polygraph examinations required by this section.”³⁹

5.0 Alternative Measures

Improved use of the existing security system. Instead of relying on polygraph tests, we advocate more rigorous implementation of current processes and improved awareness and education for both management and staff regarding subversive warning signs (living beyond one’s means, feeling unappreciated in one’s job, drinking problems, unreported foreign travel, etc.).

³⁷ Daniel Jeffreys, “Getting Down on ‘The Farm.’ (CIA’s humiliating polygraph tests are making it difficult to hire and keep operatives: reprinted from *The Independent*, Nov. 27, 1996),” *World Press Review*, v. 44, n. 3, March, 1997, p. 30.

³⁸ Robert G. Easterling, “Commentary on DOE Proposed Polygraph Examination Regulation, 10 CFR, Parts 709, 710, 711,” September 16, 1999.

³⁹ National Defense Authorization Act for Fiscal Year 2000 (Printed w/ House Amend.), S. 1059, 106th Cong. § 3168(d) (1999).

We need to recreate the DOE culture of security consciousness. Due to environment, safety, and health concerns, former DOE Secretary Watkins opened operations in the complex to such a level that an agent could more easily piece together operations at the plants. Former DOE Secretary O'Leary subsequently ordered the declassification of thousands of documents and the use of uniformly colored badges for all employees, cleared or not.

Security clearances are the first line of defense against the insider threat. However, the rigor and quality of the security clearance process has degraded through the years, for both bureaucratic and budgetary reasons. Under the Atomic Energy Commission, all employees and contractors were subject to a Q-level background investigation performed by the FBI. Today, uncleared investigators do background checks and L-cleared administrators manage the database of clearances. Clearly, the present system needs greatly increased rigor. We need more Q clearances in the laboratories. We also need more Q clearances outside the laboratories (e.g., for background investigators and DOE database administrators).

In addition to the requirement for a security clearance, the laboratories operate under the DOE policy of an employee's "need to know." This security principle requires that access to classified matter be limited to persons who possess appropriate access authorization and who require such access (need to know) in the performance of official duties. The Seniors believe that the need-to-know processes must be improved by increased use of Sigma levels, compartmentalized information, and code words for specific categories of information.

If the polygraph screening proposed by DOE is implemented, it must be integrated with the existing system of assessing the reliability of people who do weapons work. That system includes recruiting and hiring selectively, having a clearance process, doing periodic clearance updates, and asking managers to be vigilant for deviant behavior. Although the existing system is not perfect and its reliability is difficult to quantify, we doubt that polygraph screening will improve this system.

New security system requirements. Cyber security in particular needs to be improved throughout the national defense complex. Recent news regarding Moonlight Maze (where the Russians are suspected of computer hacking "sensitive military secrets, including weapons guidance systems and naval intelligence codes ..."⁴⁰) highlights the need for improvement.

We believe that the entire national laboratory security system should be improved using a systems approach in which the cost and benefits of changes can be measured. Valid indications of security levels and continuous improvement would result. A full systems evaluation is necessary because computer technology has fundamentally changed threats to national security.

⁴⁰ Ron Edmonds, "Russian hackers steal US weapons secrets," *Times Newspapers Ltd.*, July 25, 1999.

Preventing compromise of information by individuals having custody is extremely difficult. Individuals can, if necessary, memorize documents and transcribe them at home. Therefore, we must ensure that a single insider (the most common subversive profile) cannot steal “the whole store” or some large subset of it. Techniques for preventing such extended compromise include strengthened need-to-know processes and cyber and physical security techniques to minimize the possibility that an individual with limited access to data can expand that access.

Paul Robinson provides an apt summary of the situation:

In my estimation, the counterintelligence program addressing laboratory espionage must become much more sophisticated if it is to be effective. An insider spy at the laboratories is likely to be a Ph.D. in a technical discipline and possess advanced knowledge of computer systems and their vulnerabilities. It will be important for DOE to work in close partnership with the FBI and other law-enforcement and intelligence agencies on methodologies for detecting and apprehending such spies.⁴¹

The Seniors believe that internal advisory committees and red teams should be used. Other alternatives (such as more stringent physical and cyber security, sting operations, and increased surveillance) might be considered. However, alternatives must possess an intellectual foundation that can win acceptance by the scientific community in the laboratories. We believe that polygraph-screening tests are being implemented to mollify Congress—not as a viable part of a security system.

6.0 Conclusions

The Seniors find no scientific or programmatic justification for polygraph screening of employees. In fact, we believe that if polygraph testing is implemented by DOE, national security is likely to decrease by (1) making it easier for subversives to become insiders, (2) driving away talented workers and making it more difficult to recruit new workers, (3) wasting resources trying to correct the errors caused by polygraph testing, and (4) reducing employee commitment (a very important factor in national security and protection against subversion).

Countermeasures and false negatives. Most psychology experts believe that skilled subversives can use countermeasures to defeat polygraph tests. Countermeasures are a serious concern because false negatives give adversaries easier access to information. The potential for false negatives may also give the laboratories an unwarranted sense of security. Because of countermeasures, we don't think that polygraph examinations will accomplish DOE's intent—to deter or detect subversive individuals.

⁴¹ C. Paul Robinson, Sandia National Laboratories, “Testimony before the Senate Select Committee on Intelligence,” July 14, 1999.

Accuracy. Reasonable accuracy can be expected for adequately controlled, specific-incident tests. However, it is unwarranted to assume these accuracy rates for screening applications, where accuracies have not been proven to be much better than chance.

False positives. The mathematical chance of incorrect identification of innocent persons as deceptive (false positives) is high in screening applications because only a very small percentage of the group being screened might be guilty. Many innocent individuals will have careers damaged by testing and the relationship between this cost and benefit is not evident. "Tuning" polygraph tests to decrease positive results increases the probability of false negative results, and further reduces its effectiveness in identifying subversives. No technical evidence supports the contention that false positive rates can be as low as 2%. Furthermore if rates are this low, it is doubtful that any subversives will be caught or deterred.

Security system. The entire security system should be improved using a systems approach in which the cost and benefit of changes can be measured. The system should be able to be prototyped, have mechanisms to measure its effectiveness, and be amenable to improvements. A real "service in the national interest" would be to define such a security system that improves national security in both the short and long term.

Appendix I: Acronyms

ANS	Autonomic Nervous System
CIA	Central Intelligence Agency
CQT	Control Question Technique
DOE	Department of Energy
EPPA	Employee Polygraph Protection Act
FBI	Federal Bureau of Investigation
OTA	Office of Technology Assessment

Appendix II: References

Norman Ansley, "The Validity and Reliability of Polygraph Decisions in Real Cases," *Polygraph*, v.19, 1990, pp. 169-181.

N. Ansley and M. Garwood, *The Accuracy and Utility of Polygraph Testing*, US Department of Defense Report, Washington, DC, 1984.

Jeff Bingaman, "Proposed Department of Energy Polygraph Examination Regulation," Memo to Secretary Bill Richardson, September 16, 1999.

Comparison of Psychophysiological Detection of Deception Accuracy Rates Obtained Using the Counterintelligence Scope Polygraph and the Test for Espionage and Sabotage

Question Formats, Department of Defense, Fort McClellan, AL, Polygraph Inst. Report No.: DODPI93-P-0044; DODPI-R-0008, June, 95.

Dawson et al., "The Electrodermal Response," *Principles of Psychophysiology—physical, social and inferential elements*, J. T. Cacioppo and L. G. Tassinary, Eds., 1990.

DOE Cover Letter for "Issuance of Notice of Proposed Rulemaking on Polygraph Examination Guidelines," Mar. 11, 1999 (DOE Notice 472.2 extended to include contractor employees).

Pete Domenici, "Domenici Concerned Over Polygraph 'False Positives,'" Press Release, www.senate.gov/~domenici/press, August 6, 1999.

Robert G. Easterling, "Commentary on DOE Proposed Polygraph Examination Regulation, 10 CFR, Parts 709, 710, 711," September 16, 1999.

Ron Edmonds, "Russian hackers steal US weapons secrets," *Times Newspapers Ltd.*, July 25, 1999.

C. R. Honts, D. C. Raskin, and J. C. Kircher, "Mental and Physical Countermeasures Reduce the Accuracy of Polygraph Tests," *J. Appl. Psych.*, v. 79, n. 2, 1994, pp. 252-259.

W. G. Iacono and D. T. Lykken, *J. App. Psych.*, v. 82, 1997, pp. 426-433.

Daniel Jeffreys, "Getting Down on 'The Farm.' (CIA's humiliating polygraph tests are making it difficult to hire and keep operatives: reprinted from *The Independent*, Nov. 27, 1996)," *World Press Review*, v. 44, n. 3, March, 1997.

Eli Lehrer, "Lies, Damned Lies and Polygraph Tests," *Insight on the News*, v. 14, n. 28, August 3, 1998.

D. T. Lykken, *A Tremor in the Blood*, Plenum Press, NY, 1998.

James Matte, *Forensic Psychophysiology Using the Polygraph*, J.A.M. Publications, 1996.

National Defense Authorization Act for Fiscal Year 2000 (Printed w/ House Amend.), S. 1059, 106th Cong. § 3168(d) and § 3187(d) (1999).

Robert L. Park, *What's New*, Washington, DC, Jun. 25, 1999.

Polygraph Examination Regulation, *Federal Register*, v. 64, 45062 (1999) (to be codified at 10 C.F.R. pts. 709, 710, and 711) (proposed Aug. 18, 1999).

C. Paul Robinson, Sandia National Laboratories, "Testimony before the Senate Select Committee on Intelligence," July 14, 1999.

Scientific Validity of Polygraph Testing: A Research Review and Evaluation, Office of Technology Assessment (Henceforth called the OTA Report), November 1983. (available at <http://www.wws.princeton.edu/~ota/disk3/1983/8320.html>).

David Wise, *Nightmover*, Harper Collins, 1995.

Mr. UPTON. Thank you very much.

Dr. Browne. By the way, as in the first panel, your entire statement will be made a part of the record. Thank you.

TESTIMONY OF JOHN C. BROWNE

Mr. BROWNE. Good afternoon, Mr. Chairman. I am John Browne, Director of Los Alamos National Lab, and I am pleased to have the opportunity to provide your subcommittee with a statement on the status of security programs at our laboratory. I have been Director for not quite 2 years. And during that time, security has been one of the main focus areas that I've identified for improvements at our laboratory. It has been one of my top priorities.

The recent DOE audit confirmed that we've made significant progress in upgrading our security programs during the last several years, but it's clear to me that there's still many improvements that need to be made. As Dr. Robinson mentioned, security is integral to accomplishing our mission, and we recognize that the security threats that we face today are different from those during the cold war. And as such, our responses have to be continuously improved to address the newly emerging threats.

To meet these threats, I have reorganized our security and counterintelligence programs and hired new leadership to provide us with the best program possible. And I think I'm starting to see the results of having both new programs and new people in place.

I want to point out just a few things that I think are very important. First, discuss personnel security since people are the heart of anything related to security, whether it's information or materials control. And I think perhaps the most fundamental change in our security posture during the last 2 years has been the increased buy-in and involvement of our staff and our employees. Although the employees have always taken security seriously, the new challenges that we face have been met with an increased commitment at the laboratory.

To help the employees understand the threat and their responsibilities for security, we've significantly improved our employee security training and awareness program. Our management team has communicated to all employees the expectations for improved individual security responsibilities. We've had experts communicate the nature of past and present threats. We have reiterated that people will be held accountable for their actions, and we have taken disciplinary action when appropriate.

In the area of access control to our site, we are implementing a more stringent badging and control system. And this new system ties together through a central computer network key information such as citizenship, clearance level, clearance status, training needed to get into any given site, so that as an individual comes up to an access point and they hand their badge to a guard, the guard not only can see the badge, they can swipe it through and find out what's up to date on everything; and we think that's going to be an important capability that will improve our security.

During the early 1990's, the number of Q clearances was reduced for cost-cutting purposes, and this action led to an increase in the number of people at the laboratory cleared at the lower L-cleared level. This mix of clearance levels has led to additional administra-

tive controls required to restrict access of L-cleared people to secret restricted data, which of course requires a Q clearance. In my opinion, this cost-saving measure actually lessened security during this period; and we would like to see an increase, as Dr. Robinson also pointed out, in the number of Q clearances for people who must work in our facilities containing secret, restricted data. We think this would definitely enhance security effectiveness.

In the 1998 annual report to the President on safeguards and security, inadequate protection of classified non-nuclear weapons parts was identified as the single biggest information security problem at Los Alamos. We have made major improvements in protecting these classified items. The number of storage locations has been reduced from 105 to 41 and will be reduced to 22 by the end of this calendar year. We have added 25 additional protective force personnel and the patrol frequency has been significantly increased.

Cyber security is the fastest changing security issue for the laboratory and the Nation. Our classified computers where our nuclear weapons work is done are totally separated from our unclassified systems. It is a true air gap that exists between the classified and the unclassified. Classified networks have no connections to the outside world except through a National Security Agency-approved encryption device.

The recent DOE audit found that our classified computer network was secure and fully compliant with DOE orders. The recent DOE audit also tested our unclassified network fire walls that we began installing in November 1998, almost a year ago. DOE inspectors could not penetrate these barriers from outside Los Alamos. However, they did find areas that we must protect against the insider threat and we are taking corrective actions to close some of those vulnerabilities.

With respect to the insider threat, I think this is probably the biggest challenge we all face. We are now allowing no electronic transfer of authorized unclassified information from our classified systems to our unclassified systems. That's been since the April security shutdown. We are doing 100 percent scanning of all outgoing unclassified e-mail and our unclassified—the "yellow network," as we refer to it, which is fire walled, is being strengthened with even stronger password protection, enhanced network scanning and switching which allows people to only remain—have access to the information they need.

Let me close by saying that we recognize that although the audit this year came out very positive in the sense that we received a "satisfactory," the opinion at our laboratory is that we want to continue to receive a "satisfactory" and that means making continual improvements in how we approach security. It is a never-ending game. You have to maintain yourself strong against new and emerging threats.

I believe we have a solid foundation to build on. I feel strongly now that I have the right people in place and they have the right attitude and we can make this happen. Thank you.

[The prepared statement of John C. Browne follows:]

PREPARED STATEMENT OF JOHN C. BROWNE, DIRECTOR, LOS ALAMOS NATIONAL
LABORATORY

INTRODUCTION

I am pleased to have this opportunity to provide your subcommittee a statement on security programs at the Los Alamos National Laboratory (LANL).

I would like to make three key points in my testimony today:

1. Security is a top priority at the Department of Energy and the Laboratory. When I became Director two years ago, security was one of my focus areas for improvement. As such, I strengthened our security and counterintelligence activities by increasing employee training and awareness, hiring new leadership to increase our effectiveness, and increasing institutional resources to fix problems.
2. We have made significant progress in upgrading our security programs during the past two years. Secretary Richardson was particularly instrumental in focusing attention to this important matter. Our security progress is documented in our own self-assessments and was recently validated by a Department of Energy (DOE) security audit. The Office of Independent Oversight and Performance Assurance performed this audit.
3. There are still improvements to be made. The recent DOE security audit confirmed the results of our own self-assessment; there were no surprises. We aggressively pursued corrective actions before, and during, the audit. The University of California and Laboratory management is committed to implementing corrective actions until all findings are addressed.

OVERVIEW

The Los Alamos National Laboratory mission is to ensure the safety and reliability of US nuclear weapons and to help reduce the threat of weapons of mass destruction. In performance of this mission, we ensure the security of our people, our information, and our nuclear materials. Security is integral to the success of our mission. We recognize that the security threats we face today are different from those during the cold war. As such, our response must be continuously improved to address newly emerging threats.

Our Laboratory, located in a relatively remote part of northern New Mexico, occupies 43 square miles. This location presents both opportunities and challenges to security. We have 158 security areas where classified work is performed. These security areas contain over 6.5 million classified documents, 75,000 nonnuclear classified weapon parts, over 2,000 classified computers, and 3 major nuclear facilities holding several metric tons of special nuclear materials.

Our Security Approach

Los Alamos uses a layered methodology to protect classified documents and materials. With our security protection, one must overcome several barriers before obtaining access to classified matter. This methodology applies to our security programs for physical security, cyber security, information security, etc. An example of this may be observed in special nuclear materials protection at our plutonium facility. The double fence surrounding this facility has a perimeter intrusion detection system (the outer layer). The second layer is the well-trained, well-armed professional guard force patrolling the facility 24 hours a day. The third layer is the armored guard post controlling access. The fourth protective layer is alarmed vault type rooms and safes within the plutonium facility.

Los Alamos has made enhancements in all these areas of security over the past two years. Using the plutonium facilities as an example, our improvements include the following:

- improved protective forces response plans for plutonium facilities—we now get there faster with more firepower,
- state-of-the-art protective masks to counter chemical threats against protective forces,
- portable explosive-detection equipment, and
- use of a special vehicle with built-in delay and denial technologies for intrasite transport of nuclear material.

Our protective forces are capable of responding to the full spectrum of threats we face. We provide an average 250 hours of intensive training per person per year using a DOE-certified program. The results are exceptional. Over the past two years, 98.5% of the protective force have passed the critical performance tests on the first attempt. Performance is tested in areas of firearms, physical fitness, handcuffing, and unarmed defense techniques.

In August, the DOE's Office of Independent Oversight and Performance Assurance performed a comprehensive security audit. This audit inspected the five major security areas: program management, information security, cyber security, nuclear material control and accountability (MC&A), and personnel security. The DOE overall security rating for the Laboratory was Satisfactory, the highest possible rating. More importantly, this audit confirms that our corrective actions are effective. General Habiger, the DOE's "Security Czar," commented on this audit while visiting LANL on September 17, 1999. General Habiger stated: "Los Alamos just came through an evaluation with an overall satisfactory, which is the highest rating you can get, and this... was deemed the best evaluation in the history of Los Alamos. That's a phenomenal achievement."

We have structured this testimony to follow the categories used by DOE for their audit. I will now discuss the actions we have taken which contributed to receiving this overall Satisfactory rating.

PROGRAM MANAGEMENT

In April 1998, I reorganized all security functions into one division. At the same time, we began implementing Presidential Decision Directive 61 and established an independent counterintelligence program. I hired experienced professionals to lead both organizations. A former United States Air Force security officer, a specialist in running complex nuclear security organizations, leads the Security Division. The Internal Security Office is responsible for our counterintelligence program. Leading this office is a retired Federal Bureau of Investigation special agent with 30 years of field and staff experience in counterintelligence. We have continued to add external expertise to staff of both organizations. Additionally, the University of California strengthened its national laboratory security oversight by hiring a safeguards and security manager. This professional is a former United States Air Force officer who specialized in investigative programs involving computer security, personnel security, asset protection, anti-terrorism, and vulnerability assessment.

Since 1996, the Laboratory has been augmenting security funding by 10 percent per year in our overhead budget to address new demands. We increased the annual security budget from \$44 M to \$64 M. We increased the protective force by approximately 70 uniformed personnel, for a total of 390. Eight new armored vehicles were purchased to replace antiquated vehicles, and \$1.5 M was invested in a new radio system that provides improved and flexible protective force communication.

Perhaps the most fundamental change in our security posture has been the increased buy-in and involvement on the part of our employees. Employees have always taken security seriously, but new challenges have been met with increased commitment at the Laboratory. Direct involvement by our management team has communicated to all employees the expectations for improved individual security responsibilities. We reiterated that people will be held accountable for their actions and have taken disciplinary action when appropriate. Secretary Richardson ordered two security immersion stand-downs this year. Both were very effective in increasing employee awareness of the changing threats and employee responsibilities for security.

Additionally, Laboratory management continues to track and correct identified security issues. For tracking, management uses a comprehensive database system called "The Red Book." This book includes all findings and their status from every self-assessment, DOE audit, and Government Accounting Office report, plus a variety of Presidential and Congressional commission reports.

INFORMATION SECURITY

In the 1998 [DOE] Annual Report to the President on Safeguards and Security, inadequate protection of classified nonnuclear weapons parts was identified as the single biggest information security issue at Los Alamos. Los Alamos has made major improvements in protecting these classified items. Examples of our improvements include the following:

- Storage locations have been reduced from 105 to 41. This number will be reduced to only 22 locations by the end of this calendar year.
- Storage locations have been organized into security clusters. To protect these clusters, 25 additional protective force personnel were assigned to augment the existing forces.

In another area of information security, classified documents, Los Alamos was judged to have effective document control and protection over the millions of classified documents maintained at the Laboratory. DOE security audits since 1994 have validated this result. Equally important, our strategies for securing special access

programs and intelligence information have been closely scrutinized in numerous inspections and determined to meet all requirements.

CYBER SECURITY

Cyber security is a critical element of the Laboratory's overall security posture. The Laboratory maintains classified and unclassified computer networks. The classified computers are totally separate from unclassified systems—a true air gap. The classified networks have no connections to the outside world except through National Security Agency—approved encryption devices.

The following list highlights important accomplishments in Los Alamos's cyber security:

- During the recent DOE audit of security, the classified computer network was determined to be secure and fully compliant with DOE orders.
- This audit also tested the unclassified network firewalls. DOE inspectors could not penetrate these barriers from outside Los Alamos.
- Los Alamos fully participated in two security stand-downs directed by the Secretary of Energy this past spring. Extensive training on security and threat awareness was provided to the employees and contractors.
- A nine-point Tri-Lab Action Plan to improve cyber security was written and an implementation plan was approved. To date, Los Alamos has met all milestones.
- Controls to prevent any unauthorized classified-information transfer from classified to unclassified computer systems were strengthened, and an action plan for technical prevention is in place.
- No electronic transfer of authorized unclassified information from classified systems to unclassified systems has been permitted since the security stand-down. New controls, including a revised two-person information control policy, are in process of development and approval.
- Scanning outgoing unclassified e-mail and computer files for possible classified information was initiated and is ongoing.
- A stronger and improved certification program was implemented for those foreign nationals who require access to unclassified computer resources as part of their job. These foreign nationals must meet stringent programmatic criteria before access is granted. Their computer access is subject to additional monitoring and management review.

Los Alamos continues to upgrade its cyber security to adapt to changing technology and meet continuously evolving threats.

MATERIAL CONTROL AND ACCOUNTABILITY (MC&A)

Our nuclear material control and accountability needed improvement in past years. After taking corrective actions, we now have a great deal of confidence in our inventory accuracy. More importantly, our control measures have been strong, and we are equally confident that our material has been adequately safeguarded from theft or diversion.

In the 1998 [DOE] Annual Report to the President on Safeguards and Security, we received a Marginal rating in MC&A. The issue identified in that report questioned our ability to ensure that nuclear materials were in their authorized locations and at stated quantities. Much of this issue dates back to old measurement practices tied to imprecision in previous generations of measurement equipment. Through a comprehensive program involving new equipment and new procedures, we have revised and rebuilt our MC&A program. Within the last two years, our MC&A program has achieved a new level of performance that was rated by the most recent audit team as “the best in the DOE complex.” Los Alamos has been a leader in international safeguards technology for close to 30 years. We are proud of our improved internal practices to meet the MC&A standards.

PERSONNEL SECURITY

People are the heart of information control. We have increased employee security training and awareness. Additionally, we have improved our security procedures, and we are tracking and correcting deficiencies. The positive results of our effort were validated in the DOE audit. Clearance processing, human reliability programs, and security badging were determined to be operating effectively, with no findings identified.

Los Alamos continues to improve personnel security. For example, we are implementing a more stringent badging and access control system. This new system ties together, through a central computer network, key information such as current training status, citizenship, clearance level, and clearance status for each employee

and visitor. This enhancement will improve our real-time ability to tie security-area access to virtually all of the eligibility requirements for area entry. We also are installing electronic badge readers at all manned entry posts so that we have an electronic screening of each badge as well as a physical check. Our access controls also include the most extensive use in the DOE complex of collateral biometrics checks (hand-geometry readers) for access control. In addition, we have begun rebadging the entire workforce to move to the new color-coded DOE badge that will allow employees and security officers to more readily identify a person's clearance level.

During the early 1990s, there was a well-intended DOE objective to reduce the number of Q clearances for cost-cutting purposes. This action led to an increase in the number of people at the Laboratory cleared at the lower L level. This mix of clearance levels has led to additional administrative controls to restrict access of L-cleared people to secret restricted data (which requires a Q clearance for access). In my opinion, this cost savings measure has lessened security. We would like to see an increase in the number of Q clearances for those people who must work in our facilities containing secret restricted data. This change would enhance our security effectiveness.

FOREIGN VISITS AND ASSIGNMENTS

All foreign nationals visiting or on assignment to the Laboratory require prior DOE or DOE-delegated approval. In March 1999, we implemented a new internal policy that established a rigorous approval and verification process to support our foreign national visits and assignments. Every visitor has a Laboratory host, who is trained, briefed, and debriefed on the visit. The recent DOE audit verified this process through performance testing and interviews. Additionally, the auditors attempted to infiltrate foreign national "actors" into our security areas on several occasions, using false badges, ruses, and intervention by "co-opted" senior managers—the actors failed to gain access in every case. Strict access limitations are in place and verified by our Operations Security staff.

AREAS FOR IMPROVEMENT

Despite our recent documented successes, we recognize further work is required to maintain the appropriate level of security at the Laboratory. Significant examples include the following:

- We will continue to expand and improve the comprehensiveness and quality of our security-training program. Clearly, our employees are our first and best lines of defense in meeting the tremendous challenge of safeguarding nuclear material and classified information. Training is the key through which we keep our employees knowledgeable of and vigilant to security threats. We have a number of initiatives underway, which are relevant and meaningful to our mission and the security challenges we face.
- We will continue our efforts to protect against the insider threat to our cyber security. Our efforts will be coordinated with the IsecM Task Force, which is composed of representatives from the three nuclear weapons laboratories, the DOE nuclear weapon production plants, and the DOE.
- We recently obtained release of funds from DOE for the first segment of our Nuclear Material Safeguards and Security Upgrades Project (NMSSUP), which is intended to replace our aging security alarm system. We will work to ensure this line-item construction project is accomplished within scope, schedule, and budget. We have assigned one of our best project managers to this project, and it receives regular review by my senior managers and me.
- We have added an effective firewall to protect our unclassified network. We will continue to expand the vulnerability testing of these unclassified computer systems to ensure our systems are adequately protected from within the firewall (the insider threat).
- We will reduce the use of temporary nuclear material access areas. Our older facilities require the occasional use of temporary material access areas. These areas are created to utilize specialized equipment outside the normal special nuclear materials protective area. These temporary areas provide full protection for the nuclear materials. However, they are more difficult to protect and require expensive compensatory measures. Minimizing the use of these areas and obtaining newer secure facilities are the best solutions to this issue.
- We will continue to improve our internal Laboratory coordination between counterintelligence, security, and foreign visitor and assignment organizations.

CLOSING REMARKS

I am very pleased that the recent DOE security audit recognized many improvements to the Los Alamos security programs. In those areas identified for further improvement, I want to assure you that we are committed to making those improvements. We are committed to continuous improvement of our security program, just as we are with safety, facilities, project management, and other areas of business and operations. We have a solid foundation to build on, we have a detailed plan for the path forward, and most importantly, we have the right people, with the right attitude, to make it happen. I would like to thank Secretary Richardson and other DOE leaders for their support of our Laboratory's efforts to improve security. With the continued support of the administration and Congress, we will continue to achieve established security goals.

Mr. UPTON. Thank you very much.

Dr. Tarter. Welcome back.

TESTIMONY OF C. BRUCE TARTER

Mr. TARTER. Thank you, Mr. Chairman. Let me begin by saying, in partial answer to a comment Mr. Podonsky made this morning, we are responding to 100 percent of all of the findings which were found in the OS&E inspection. Let me briefly comment on our response in the three areas that I've discussed before: physical security, computer security and then personnel security.

In the area of physical security, I think the three major areas in which there were significant findings, I think the most important, as alluded to earlier by, I believe, Congressman Cox, was essentially on the Superblock and the guarding of special nuclear material. And I think—as Mr. Podonsky said this morning, I think we have done a number of things. We have done a very, very large number of computer simulations to test all kinds of scenarios for possible intrusion into that area. And I think those have—I think exposed and allowed us to take measures to work on that facility.

I think we carried out a physical force-on-force exercise during September, which again will have to be judged eventually by his team, but I think we did it in concert with the Oakland operations office, with the defense programs office in DOE, and I think, learned a great deal; and I believe we were reasonably satisfied with the results of that exercise.

The third piece, which I alluded to in my July response, we have been adding special response team personnel and they basically go through extensive training. The first new class I believe will graduate this December, and then the other classes will soon come on line, which will bring us to full strength in terms of the special people to respond in those areas.

In terms of the materials control and accountability overall, we have essentially completed, in our judgment, the work in all but one area; and as was discussed this morning, that last area involved acquiring measurement capability, which we have basically done this week, and we will begin to use that to take measurements on the inventories in this one area, which I don't want to go into further in an open hearing, but that will be well under way.

Finally, in the classified part of physical security we expect to have all of our storage areas brought into the standard configurations by the end of the year, and we're using special patrols to guard that during the interim until we have done that.

In the area of computer security, I think our major activity both in response to the Secretary's 6-point plan and the 9-point plan,

but also the findings, is to bring a very extensive new fire wall into operation in the unclassified part of our systems. A second—and that's acquired, but it will take extensive work to separate into all of its components; and that is where we're putting much of our effort.

The other activity I would mention, in which all three of the laboratories are participating, and which I think Dr. Weigand could comment on further, is that all of the labs and external experts in computer security have basically spent a great deal of time trying to assess all of the conceivable measures. And this is done in concert with things like the National Security Agency and the other parts of the government which have to work at high levels of cyber security; and I think we have carried out an extensive set of discussions and workshops with a number of recommendations for cyber security in general, but I would rather let Dr. Weigand, or perhaps Dr. Gilligan, comment on how those are going to be responded to and how they will fit into the 6- and 9-point plans.

Let's see. In terms of the foreign national access, which was clearly a topic of significant discussion this morning, we have tightened the administrative controls along the lines General Habiger indicated so that we have even more extensive—we have always had an extensive review process for the foreign national access, but we have added layers of additional review before any foreign national has access to the computer site.

Finally, I will just mention briefly in the area of personnel security, I think, as both Dr. Robinson and Dr. Browne have commented, that a significant issue for us has been the presence of L clearances. I think we have asked again for Q clearances; I think we're pleased—we would like to have an all-Q site. In the first proximation—in the interim, we have added a number of physical barriers so that it is not—so that L-cleared people cannot simply administratively and easily get into the Q areas as an interim measure. But I think our preferred result is to have essentially a Q-cleared facility inside a Q-cleared—basically inside the restricted areas. I think we are—for all kinds of reasons we think that was a vulnerability, and we think changing that will enhance the security of the site.

Finally, in response to another comment this morning, we have used polygraphs. We have not done them as part of the new CI program, but they have been used historically as part of the investigative process, and so the tool has not been part of the systematic thing, but has been part of the investigative process used with staff members in the past.

And so I will leave that with that, and I will be happy to take questions again from the staff.

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

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

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. In my testimony to this committee on July 20, 1999, I stated our commitment and described our efforts to provide increased confidence in the security of the Laboratory. I would like to report to you today the substantial progress that has been made in addressing the issues resulting from the May 1999 inspection by the DOE Office of Security Evaluations (OSE).

In the area of protection of Special Nuclear Materials (SNM), we are well along in executing an action plan to analyze, document, performance test, and enhance the Laboratory's comprehensive protection strategy. There have been several progress reviews by DOE Defense Programs (DOE/DP) and the Oakland Operations Office (DOE/OAK). Hundreds of simulations have been performed, and a force-on-force performance test against an outside adversary team has validated the protection strategy. In parallel with this effort, there have been numerous physical and procedural upgrades and interim staffing increases. A new class of Special Response trained officers will graduate in December and enhance our staffing.

In the area of Materials Control and Accountability (MC&A), we have demonstrated the ability to consistently meet SNM measurement and inventory requirements and resolve inventory differences in a timely manner. Specific concerns raised by the OSE, ranging from statistical sampling procedures to verification of tamper indicating devices, have been addressed. This past week LLNL took delivery of a new certified calibration standard from DOE's New Brunswick Laboratory that will allow us to begin making certain specific accountability measurements.

We have also made improvements in the area of physical security and protection of classified matter. Performance issues identified by OSE in several vault-type rooms (VTRs) have been corrected, and two newly-hired alarm testers are conducting a detailed inspection of all vaults and VTRs at the Laboratory. Alarming and other physical upgrades of non-compliant classified parts storage areas are being aggressively pursued and will be completed by the end of the year. Over 100 non-GSA-approved repositories have been replaced, and we are in the process of replacing or relocating the remainder to VTRs. Physical barriers have been installed in many Q-clearance-only areas to restrict accidental access by L-cleared personnel, and a comprehensive cost and engineering study for completing the remainder is nearing completion.

The Laboratory has taken many steps to improve cyber security. Computer access by any foreign national must be approved through a rigorous review process. For cases where dial-in access is allowed for foreign nationals, the access is routed through a single terminal server running state-of-the-art network intrusion detection software. In addition, unclassified systems are being scanned for vulnerabilities, and outgoing e-mail is being scanned for classified content. No issues have arisen. Steps have also been taken to limit the physical possibility of accidental transfer of information from a classified system to an unclassified system. We have installed a firewall between the open and restricted partitions of the unclassified network and are beginning transition of servers to the appropriate partition. And finally, we are actively participating in the DOE/DP Integrated Security Management (ISecM) initiative to further improve computer security.

In summary, much progress has been made in addressing the issues identified by the DOE/OSE security evaluation, and we are well on our way to reaching the goals we have set. I am committed to achieving an excellent Safeguards and Security Program at the Laboratory.

PROGRESS ON OSE FINDINGS

Protection Program Management

During the inspection in April, DOE/OSE (now DOE Office of Independent Oversight & Performance Assurance, DOE/OA) cited a concern that LLNL had not demonstrated assurance of the SNM Protection Strategy. Immediately, LLNL responded with a "Path Forward" action plan to analyze, document, performance test, and enhance the Laboratory's comprehensive protection strategy. With the support and concurrence of DOE/OAK, DOE/DP and DOE/OA, LLNL has performed over 300 tabletop and computer modeling simulations of possible adversary scenarios. The results provided LLNL with the credible scenarios that were performance tested during the first two weeks of September. During the week of September 12, DOE/OAK validated and DOE/DP verified the LLNL protection strategy through force-on-force testing conducted with an outside adversary team. The validation and verification testing was observed by representatives of DOE/OA and the Office of Security and Emergency Operations (DOE/SE). General Habiger was present for part of the validation and verification exercise.

LLNL will implement the new protective force posture in December 1999, when a new group of Special Response Officers graduate from their SPO III Academy training. In the interim, increased protective force personnel are staffing the facility around the clock. Significant physical and procedural upgrades developed during the Path Forward analysis and performance testing have been implemented, with other upgrades on target for completion in February 2000.

Material Control and Accountability

LLNL has made great strides in achieving its commitment to the DOE Assistant Secretary for Defense Programs to rectify all MC&A issues, including those cited in the Annual Report to the President on Safeguards & Security and those of the DOE/ OSE inspection report. Of the seven issues, all but one has been closed and validated by DOE/OAK. In particular, LLNL's MC&A team has demonstrated the ability to meet DOE's requirements for SNM measurements and inventory monitoring. The team has implemented procedures that are able to quantify and resolve inventory differences within a prescribed time frame and that process has been validated. Other validated procedures include means for assuring that personnel removed from the Personnel Assurance Program (PAP) and the Personnel Security Assurance Program (PSAP) are not permitted access to SNM, providing inventory confirmation of in-process material, and verifying the integrity of tamper indicating devices. In addition we have developed an improved sampling plan, based on item attractiveness, to be used to confirm inventory.

The Laboratory has now received shipment of certified measurement standards from New Brunswick Laboratory for use in inventory and measurement accountability. These standards will enable LLNL to begin certain accountability measurements by the close of 1999.

Physical Security

The physical security program at LLNL was rated satisfactory; however, DOE/ OSE identified five areas of weakness. Two of the concerns were addressed through modeling and performance tests as part of the Path Forward activity for Protection Program Management. LLNL's final protection strategy, which was validated by DOE/OAK, mitigated those concerns. One of the remaining concerns was closed through updated operational directives and was validated by DOE/OAK.

One of the remaining issues relates to the protection of classified matter and the adequacy of sensor coverage and proper testing. LLNL has taken aggressive action to address this concern. Two additional alarm testers have been hired and all alarm testers have now completed formal physical security training through the DOE Non-Proliferation and National Security Institute. The VTRs that were questioned in the OSE report have all been brought into compliance and there is an aggressive schedule to inspect and test all other VTRs and vaults at LLNL by the end of the calendar year.

The other remaining issue deals with the barrier delays for SNM laboratory doors. The validated protection strategy uses the delay value of the existing doors and basically mitigates the need for doors with longer delay times. The existing doors are not in compliance with the current DOE order. LLNL is developing a project plan, including a cost/benefit analysis, for the replacement of the doors to meet the DOE standard.

Classified Matter Protection and Control

In the area of the protection of classified matter, LLNL took immediate action to mitigate the OSE's concerns regarding the non-standard storage of classified parts. We established a two-hour roving protective force patrol for the identified storage areas and now are fully compliant with pertinent DOE Orders. In addition, LLNL has completed a comprehensive self-assessment to assure that all facilities housing non-standard storage of classified parts, including those identified during the OSE inspection, are appropriately protected.

LLNL has initiated an aggressive upgrade program to bring all identified areas of non-standard storage to either the VTR standard or to relocate the items to vaults or VTRs by December 15, 1999. That program is well under way with alarm and physical upgrades currently being installed and items being consolidated or destroyed.

LLNL has identified all the locations of non-GSA-approved repositories and a comprehensive plan to replace all non-GSA repositories not stored in VTRs has been initiated. The plan also includes bringing into operation a new identification method that will permit the location of all repositories to be tracked in the LLNL property management database and verified by protective force patrol checks. Over 100 new repositories have been replaced to date, with additional containers on order. It is

the goal of LLNL to either replace, relocate to VTRs, or provide off-hour checks of all non-GSA repositories by December 31, 1999.

A DOE/OSE concern was raised about the procedures and barriers used in Limited areas where personnel with both L and Q clearances have access. A survey of such areas is complete and a cost/benefit analysis is due on October 31, 1999. Options include the use of barriers and access control or requests for additional Q clearances. Many programs at LLNL have already installed, or are in the process of installing, physical barriers and access control to segregate L-cleared employees from Q-only areas. LLNL does not have any L-cleared foreign national employees. We have, however, implemented a policy to require any potential L-cleared foreign nationals from elsewhere in the DOE complex to be escorted in general limited areas.

LLNL has implemented other actions to address the OSE concerns in the area of protection of classified matter, including modification of the Laboratory's Operations Security plan to place added emphasis on the highly critical and sensitive topics.

Cyber Security

LLNL is actively participating in the ISecM initiative chartered by DOE/DP. ISecM aims to achieve a comprehensive, integrated solution to improving security in the DOE Nuclear Weapons Complex, particularly security against the "insider" threat. ISecM constitutes a major upgrade to security in the Nuclear Weapons Complex and will require several years with significant new funding to implement. When implemented, ISecM will integrate security more fully and more transparently into classified computing across the Complex. In the long term, ISecM will comprehensively address the concerns expressed by the OSE while broadly improving security in the Complex.

In the near term, LLNL has taken immediate actions to address OSE concerns. LLNL has installed a state-of-the-art system to monitor all remote dial-in access by foreign nationals. In addition, LLNL has strengthened its existing foreign national approval process. We now require review and approval by the LLNL Chief Information Officer (CIO) and the LLNL Associate Director for National Security for cyber access by any sensitive-country foreign national.

We are also vigorously addressing OA concerns related to LLNL's implementation of the Nine Point Action Plan:

- LLNL is applying Tamper Indicating Devices (seals) to classified computers to increase the assurance that users do not modify their computer systems to add ways of transferring data.
- LLNL has instituted rigorous new procedures for the authorized transfer of unclassified files from classified systems.
- LLNL is scanning all its unclassified computer systems to determine whether or not those systems have vulnerabilities.
- LLNL has procured new software that has the potential to significantly increase the Laboratory's ability to automatically scan e-mail for classified information.
- LLNL has installed a firewall between the open and restricted portions of the unclassified network and is beginning transition of servers to the appropriate partition. The firewall will be fully operational by March 1, 2000.

In addition, LLNL's programs have re-evaluated the need-to-know boundaries pertaining to the information they handle and their personnel. Each LLNL program area is restructuring its computer systems appropriately to enforce more stringent need-to-know separations.

To guide computer security in the future, the Laboratory has created a Computer Security Policy Board headed by the LLNL CIO to promulgate policy regarding computer security for the site.

CLOSING REMARKS

The security evaluation conducted by OSE noted many improvements to LLNL's security system while identifying areas for further improvement. We are carrying out a comprehensive corrective action plan to address those areas, and much progress has been made. I have committed the resources and set priorities to ensure that this plan is executed. Many corrective action milestones have already been achieved, and we are on schedule with the remainder. Most milestones are expected to be achieved by the end of the year. DOE has evaluated and concurred in or validated much of our work to date. OA has noted LLNL's strong commitment to action.

I appreciate the opportunity to provide an update to the Committee on the status of security improvements at LLNL. I am confident that our Special Nuclear Material and sensitive and classified information are secure.

Mr. UPTON. Thank you very much.

Dr. Weigand, welcome back.

TESTIMONY OF GIL WEIGAND

Mr. WEIGAND. Thank you, again. I would ask that my full text be entered into the record, and then I will attempt to be extremely brief and you can get on with the questioning.

I do appreciate the opportunity to appear before the committee again. I want you to know that as I have indicated before I am fully committed to strengthening the security posture at the laboratories and in defense programs, and doing so by the end of the calendar year. I hope to achieve a "satisfactory" rating on the report that goes back over to the President.

You are fully aware that last year's report that went to the President did not have a "satisfactory" rating, it had a "less than satisfactory"; and as a result of that, the Assistant Secretary, along with the cooperation of Deputy Assistant Secretaries like myself have created a set of corrective action plans and reported those corrective action plans to Under Secretary Moniz in a memo we call the "goalpost memo."

It is a classified memo in which we lay out the plan by which we expect to achieve our "satisfactory" rating by the end of the year. It was clearly based upon the information we had at the time we drafted the memo.

I think why I am very confident that we are going to come to this "satisfactory" rating or very close is because the three things it takes to make this happen are in place. One, there is a corrective action plan. That corrective action plan two, has milestones, measurable; if not week-by-week, they are appropriate, and they are reported to my office on a regular schedule. And we can audit those a bit.

And third and most important is that a corrective action plan with milestones and clear objectives is one thing, but funding it is the other. And this plan has been funded. I have letters from each of the directors of the laboratories that they will fully fund those corrective action plans.

I think on the positive side here, we have just recently gone through a set of inspections by the independent office. Those inspections, as you have heard today from Mr. Podonsky, are showing very good progress, very good signs we had an overall satisfactory rating at one of the laboratories, Los Alamos, and we are very proud of that progress.

One other thing I did want to mention here is that we aren't just leaving this to a goalposts memo that ends at the end of this December. Those are what I call the intermediate set of actions.

I have asked the laboratories to form a laboratory-industry task force to create a plan for continuous improvement. The purpose of the plan is to ensure that our security will be sustainable in the long run and capable of adapting to the threat as it increases. And I really want to emphasize that. This is not a game where the threat lies dormant and lets you have some slack. This is a slippery pole. As you climb and achieve new technological advances to overcome the current threats, those technologies are used against you in the future to overcome the barriers you put up.

So this is a slippery pole on which we have to constantly be climbing. I am very interested in the continuous improvement.

I asked this task force to work jointly with myself and the Office of the Chief Information Officer, Mr. Gilligan, who is here with us today. If you wish to question him, I am sure he will be willing to offer his viewpoints.

I also charged this task force to make cyber security within defense programs "best in class." We would do as good as the rest of the government and hopefully adapt what good ideas they use throughout the government. But I insisted they take one additional step, and that is that I wanted them to be very forefront on insider espionage. I think that is a capability that the Department of Energy could contribute across the government. Given the concern of this committee on insider espionage, I think that we need to step up to that, and I ask the committee to do that.

To ensure objectivity in this task force, I established a leadership team that was chaired by Bill Crowell, who is the Chief Executive Officer of Cylink and the past Deputy Director of the National Security Agency. The majority of the leadership team was selected from commercial enterprise, including Boeing, IBM and TRW who have a very large enterprise in classified work for the Federal Government, IBM and TRW. The TRW representative was Bill Studeman, Admiral Studeman, was the former Deputy Director of the Central Intelligence Agency.

I stacked this committee in favor of the industry representatives who knew the cyber security world from inside the government and outside the government. They can outvote the labs at any given time.

The task force proposed a long-term system-level approach to cyber security and provides a basis for creating the 21st century classified information system for defense programs that will continue to enhance the protection of our classified and sensitive nuclear weapons information, on ongoing and increasing threat.

We have a draft from them. We are evaluating that draft. We are looking at options on how to implement and options on how to fund. And, again, because this is a system-level approach that we are taking here, it has many nuances to it, and we need to assess them fully before we get back to the committee with what we think we should be doing.

So, in conclusion, I just believe there has been significant progress. I think you have a pretty good team in place right now. I think we just need to move the ideas and the plans that we have forward, and hopefully by the end of this year we will be reporting back to you a "satisfactory" along with our report to the President with a "satisfactory."

[The prepared statement of Gil Weigand follows:]

PREPARED STATEMENT OF GIL WEIGAND, DEPUTY ASSISTANT SECRETARY FOR RESEARCH, DEVELOPMENT AND SIMULATION, OFFICE OF DEFENSE PROGRAMS, U.S. DEPARTMENT OF ENERGY

INTRODUCTION:

Mr. Chairman, and distinguished members of the Committee, I appreciate the opportunity to testify on security issues. We, in Defense Programs, are fully committed to ensuring that our laboratories and facilities enhance their safeguards and security protection postures and achieve a Satisfactory rating by the end of the calendar

year. As line managers, we fully recognize that effective safeguards and security protection is required in order to meet our National Security mission. AP-PROACH:

As documented in the most recent Annual Report to the President, several Defense Programs' sites were rated less than Satisfactory. These ratings were based on previous oversight reviews (surveys, assessments, inspections). On May 24, 1999, the Assistant Secretary of Defense Programs set forth in a "Goal Post" memorandum to the Under Secretary, our get-well plan and approach to correct deficiencies by the end of the calendar year. The "Goal Post" memorandum was coordinated with Non-Proliferation and National Security and the Office of Independent Oversight and Performance Assurance and accepted by the Under Secretary. It committed to "fix the problems" through immediate and interim actions and follow-on corrective actions with associated milestones to be completed by the end of the calendar year. We have committed an abundance of resources to fix the problems and, to date, have reprioritized funding within our existing budget. Finally, we are closely tracking all Corrective Action Plans to assure milestones are being appropriately met.

Also, there have been inspections completed at Lawrence Livermore National Laboratory, Sandia National Laboratories, and Los Alamos National Laboratory subsequent to the Annual Report to the President. These inspections by the Office of Independent Oversight and Performance Assurance focused on a review of safeguards and security programs with documented problems and evaluated the effectiveness of cyber security programs in both the classified and unclassified areas. While work remains to be done, recent inspections have documented that significant progress and improvements have been accomplished at all of the weapons laboratories in the safeguards and security, as well as cyber security areas.

As you are aware, the Department has recently been giving much attention to the area of cyber security. This began with action plans to address the Secretary's nine points and six enhancements. Once the plans had been developed and implementation had begun, I asked the laboratories to create an Integrated Security Management (IsecM) Task Force. The task force was to prepare a plan for continuous improvement. The purpose of this plan is to ensure that our security will be sustainable in the long run and be capable of adapting to the threat as it increases. Specifically, I charged the task force with developing a plan that has been coordinated with the Department's Chief Information Officer to make the cyber security within Defense Programs the best in class and preeminence against the insider threat. To ensure objectivity, I established a leadership team for the task force that was chaired by Bill Crowell, Chief Executive Officer of Cylink and past Deputy Director of the National Security Agency. The majority of the leadership team was selected from commercial enterprises, including Boeing, IBM and TRW, the TRW representative being Bill Studeman, former Deputy Director of the Central Intelligence Agency.

The task force has proposed a long-term system-level approach to cyber security. It provides the basis for creating a 21st Century classified information system for Defense Programs that will continue to enhance the protection of our classified and sensitive nuclear weapons information in the face of ongoing increases in the threat. The task force completed the plan in September and is currently refining the associated cost estimate. The plan has been submitted to the Department and is currently being reviewed. I hope for a decision on further action soon.

I will now provide a brief summary of specific actions taken and planned to correct weaknesses in safeguards and security at the DP laboratories by the end of the calendar year.

LAWRENCE LIVERMORE NATIONAL LABORATORY (LLNL):

All worst case adversary paths and scenarios have been reassessed to include re-running of all computer modeling and performance tests to validate the protection posture at the "Superbloc" (where SNM is processed/stored). There has been an increase in protective force manning at the Superbloc and additional physical security upgrades have been put in place. New and enhanced procedures have been put in place and validated by Oakland Operations Office to address weaknesses in the material control and accountability area (addresses Tamper Indicating Device integrity, Inventory Differences Analysis, Inventory Sampling Plans based upon attractiveness of SNM, and acquiring reference materials for measurement of uranium holdings). In the area of Classified Matter Protection, LLNL has established two-hour patrols during off hours, holidays, and weekends of classified matter/parts pending the matter/parts being relocated to vaults or alarm system upgrades completed by December 15, 1999. All vault type room alarm coverage is being assessed with corrections by

December 31, 1999; those identified during the inspection have already been corrected. Also, additional alarm testers have been hired and trained. Lawrence Livermore National Laboratory is in the process of consolidating its classified holdings destroying unnecessary classified materials. In addition, over 100 GSA approved repositories have been received with additional on order.

In the area of unclassified cyber security, LANL is scanning E-mail to detect classified information that has been accidentally or deliberately placed in an unclassified message. Across the Lab vulnerability assessment scans are being conducted. Also, the Computer Security Organization has instituted "spot checks" to assure the vulnerability scans are being completed and to further assure that significant vulnerabilities uncovered by the scans are corrected. Finally, foreign nationals are not permitted access to a Limited Area unless under escort. In addition, intrusion detection is in place to monitor off site foreign national access to LLNL's open terminal server.

SANDIA NATIONAL LABORATORIES (SNL)

SNL has taken several immediate actions to improve security including restaffing a protective force tower position, creating an additional elevated protective force response position, and adding physical barriers at the material access portals to protect the protective force members. Additional physical security enhancements have included securing tamper switches on alarm cabinets and the implementation of metal detector procedures to detect items in shoes. In the area of materials control and accountability, SNL has updated its physical inventory and tamper-indicating procedures as well as ensuring that existing measurement plans reflect the procedure of always measuring 100% of Category I nuclear material holdings. In the area of classified matter protection, SNL has increased the frequency of protective force patrols of buildings containing classified parts and has placed a Security Police Officer in one building containing Secret Restricted Data parts during non-operational hours to perform a full perimeter walk-around. All classified containers, including space savers, have been made accessible to the protective force and SNL will provide a plan to DOE by December 23, 1999, for the approved standard storage of classified materials either in GSA safes, vaults, or vault-type rooms. Also, deficiencies in the SNL security infraction/inquiry program are being addressed with the recent addition of 3 staff members to the Security Incident Management Program Team with the elimination of the backlog of security inquiries/investigations to zero by December 23, 1999.

In the area of unclassified cyber security, SNL is moving forward aggressively to implement the Secretary's six further enhancements to cyber security. Also, SNL now has in place a formal process requiring SNL Vice Presidential approval for any foreign national access to the unclassified Sandia Restricted Network (SRN). They have also applied tamper-indicating solutions to unused ports of classified computers collocated with unclassified computers and implemented the NT secure model on the SRN servers with deployment to individualized computers by December 23, 1999. They will also correct all significant vulnerabilities on the Sandia Open Network (SON) and SRN computers as an interim measure and implement the automated NT server model with monitoring on the SON plus servers by December 23, 1999. Finally, SNL plans to implement the UNIX SECURE Model on SRN and SON by September 29, 2000.

LOS ALAMOS NATIONAL LABORATORY (LANL):

The LANL protection program was rated in the February 1999 Annual Report to the President as Marginal with all topical areas also rated as Marginal. However, the August 1999 comprehensive inspection of LANL resulted in an overall SATISFACTORY rating. This represents the commitment of senior line management to address the actions needed to correct past deficiencies and weaknesses. LANL has effectively addressed long-standing problems in the accountability of nuclear materials and has made significant progress in addressing deficiencies in the protection of classified weapons matter/parts. There have been significant physical security upgrades put in place and the protective force response has been robustly improved and performance tested. Aging security systems are being addressed by a line item construction program. LANL will be down from 105 buildings containing classified parts to 22 buildings within 8 building clusters with 8 dedicated patrols by December 31, 1999. In the area of material control and accountability, LANL is using current limit of error inventory difference data for inventory calculations and will review all nuclear material characterized as not amenable to measurement and revise, as appropriate, their plan by November 30, 1999. The inspection team characterized the LANL materials control and accountability program as the best in DOE.

In the area of unclassified cyber security, LANL has strengthened its policy on foreign national access to their unclassified network and by November 1, 1999, will assure that all systems accredited to process classified material employ tamper indicating seals on unused ports. They will also have finished by November 1, 1999 the strengthening of their pass word protection and implementation of a scanning process and on-going performance-based testing. LANL has already begun implementation of switched networks (65% completed on red, 40% on yellow networks- all to be completed by FY-2000).

CLOSING:

As you can see, significant progress has been, and continues to be, made. We are prepared to brief the Committee in more detail on the specific actions underway to meet "goal post" commitments and to correct weaknesses noted by the recent inspections. Mr. Bill Hensley is available to provide these briefings.

In closing, I want to again express Defense Programs' continuing line management commitment to improving our Laboratory and facility protection programs and obtaining Satisfactory protection programs by the end of the calendar year.

Mr. UPTON. Thank you very much. Dr. Turner?

TESTIMONY OF JAMES TURNER

Mr. TURNER. Thank you, Mr. Chairman. I have a short statement.

I am pleased to return to give you a status report on our efforts to address safeguards and security findings at the Lawrence Livermore National Laboratory. I am the manager of the DOE Oakland Operations Office. Our role in security consists of two parts: First, we provide Federal oversight of the laboratory through the presence of Federal personnel on the site and in the facilities. These Federal staff, one, perform spot checks on activities; two, conduct focused reviews and issue findings where appropriate; three, validate that corrective actions are complete and effective; and four, maintain a constant presence in key facilities to understand what is being done and to offer suggestions for improvement.

Second, I am the DOE contracting officer for the contract with the University of California for the management and operation of the Lawrence Livermore National Laboratory. In addition to administering the terms of the contract, we work with headquarters to develop performance measures and to assess the laboratory's performance annually.

When we were here in July, a corrective action plan had been agreed by the parties in the field and headquarters, several upgrades and improvements were under way, and Livermore was working cooperatively with Sandia and Los Alamos in areas of common interest, such as cyber security. At that time, Livermore was meeting all time lines and milestones in the corrective action plan. To date much more work has been completed and the laboratory is still on track with the agreed schedule.

Some examples of specific actions taken are: increasing the numbers of protective service officers within the Superblock where plutonium, enriched uranium and classified parts are stored; successful completion of performance tests to demonstrate the capability to protect Superblock assets in scenarios consistent with the design basis threat; successful completion of bimonthly inventories of special nuclear material to address previous deficiencies in nuclear materials controls and accountability; the acquisition of measurement standards for precision measurements of quantities of nuclear material—this was accelerated through the assistance of General

Habiger; increasing the number of sensors and alarms in open storage areas to protect classified parts; and implementing the Trilab cyber security plan for classified and unclassified computers.

In summary, the laboratory is still on track to complete the steps necessary to have the safeguards and security rating assessed by Mr. Podonsky's office changed from the current "marginal" to "satisfactory," that is, to have the laboratory "green" by the end of the calendar year. This is a commitment I made to Secretary Richardson. Dr. Tarter made a similar commitment. In my view, we're working hard, working well and working together to implement this commitment.

In addition, for fiscal year 2000, the performance evaluation points allocated to security in the contract have been increased such that they are now equal in weight to safety.

The final point I want to make is that we're committed to continue the pressure and the momentum to improve security against the current threat, new, emerging threats and evolving threats such as those in the cyber security area. I agree with Mr. Podonsky that security is an attitude. It is a responsibility that all of us who deal with national security and economic security matters accept when we take such positions. To be most effective, security and safety should be an integral part of the work needed to accomplish the program mission.

Thank you, sir.

Mr. UPTON. Thank you very much.

As we did with the first panel, members will be allowed to ask questions for about 5 minutes. And we will rotate between sides and probably have one or two rounds of questions.

First of all, I appreciate all of you for—those of you who testified before, certainly—coming back. And our subcommittee has had a long history, whether it be Republican or Democrat, in trying to identify abuse, going after it and then making sure that it's corrected. And I do believe that we are on the right track to correct it. I just want to make sure that we are on a fast enough track to make sure that secrets in the future will not be allowed to be given away.

And I guess, with that in mind, I have a couple of questions. No. 1, Dr. Robinson, you indicated and so did Mr. Tarter, background checks, polygraph checks have been taken—wait, maybe you didn't say so, Dr. Tarter, but Dr. Robinson, you indicated that polygraph tests had been taken from a number of DOE employees more than just the CI folks?

Mr. ROBINSON. These are laboratory employees who are involved in special compartmented programs. And to participate in those programs, agreeing to be available for polygraph was a part of the condition for joining those programs. I'm giving you the statistics on the actual number of folks who were involved in such programs, who have been called on and have been polygraphed.

Mr. UPTON. Dr. Tarter, you indicated that you wanted more Q-cleared folks as compared to L, which I assume is a lower clearance?

Mr. TARTER. Yes.

Mr. UPTON. But Q-cleared folks don't have the background check, do they? Or don't they? Do they—what is the difference between an L and a Q other than the M-N-O-P.

Mr. TARTER. Perhaps Rich Mortensen ought to come up—

Mr. UPTON. What level of degree is different for a Q than an L?

Mr. TARTER. Rush?

Mr. INLOW. I am Rush Inlow, Deputy Manager, Albuquerque Operations. A Q is a full field investigation currently done by the Office of Personnel Management in most cases. It also includes a records check and a statement from the applicant, filling out a questionnaire that deals with both background and lifestyle issues.

An L is merely a records check and a statement submitted by the applicant.

Mr. UPTON. Now, these clearances are only for U.S. Government employees; is that correct?

Mr. TARTER. No, U.S. citizens who are—

Mr. UPTON. U.S. citizens that are participating at the labs or employed at the labs?

Mr. ROBINSON. There are a few exceptions of foreign people who have obtained clearances. We have a UK employee working in a limited cleared area with a Q clearance.

Mr. UPTON. What percentage of foreign nationals that would have access to unclassified information, what type of clearance, if any, would those individuals have?

Mr. INLOW. None.

Mr. ROBINSON. They would have none.

Mr. UPTON. And they do have access; is that not right?

Mr. ROBINSON. No.

Mr. UPTON. Not even to unclassified?

Mr. TURNER. Unclassified, yes.

Mr. UPTON. But not classified?

Mr. TURNER. Correct.

Mr. UPTON. Is that 100 percent guaranteed?

Mr. ROBINSON. To the best of our abilities, yes.

Mr. UPTON. Dr. Weigand, you mentioned a goalposts memo. I don't know whether I asked our staff if we had a copy and we may have one in my—though I'm not sure. I've not seen it, though we may have it. One of the things that I indicated in my opening statement was that I think a number of members may be interested in going to see for themselves a number of the labs, probably come January when Congress is in recess and it will not interfere with our votes here.

Do you know whether the goalposts memo has been shared with our committee staff?

Mr. WEIGAND. Mr. Chairman, your staff has the memo and we would be glad to supply another copy.

Mr. UPTON. One of the things that I would ask is that before we embark on such an adventure, going to these three labs, I wonder if it would be possible for you to come up and give a briefing to those members who might be interested and go through the goalposts memo and look at the recommendations and look at the time lines that you suggested. And as you indicated in your testimony, the milestones that are there are on a regular schedule and you believe that they are fully funded, but I wonder if we might get a re-

port at that time, in January maybe, in a private meeting of those members to see how the labs in fact are doing with regard to the suggestions that you offered, to make sure that in fact we are achieving the milestones and the direction that you thought was wise?

Mr. WEIGAND. Sir, so I'm really committed, let me commit myself to do the following: Since it's on the record—I just got through looking at the cyber security, the nine points and so forth corrective action plans; and I asked for an informal audit by some of my staff to do that. And I get reports back of different things that we see happening and we are responding to some of those. I will be perfectly willing and happy to again have my staff informally meet with the laboratories and find out exactly where they stand on these corrective action plans.

To my knowledge, they are on time and sort of on schedule, but there are always little concerns here and there that come up, and I'll be glad to share that with your staff before you go out.

Mr. UPTON. Thank you.

Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. Browne, you became director of Los Alamos lab in 1997; did you not?

Mr. BROWNE. That's correct. November.

Mr. STUPAK. I had a couple of questions about the Wen Ho Lee investigation, and I would like to ask you, since you're here today, when were you first briefed about this investigation?

Mr. BROWNE. It was about 2 weeks after I became Director.

Mr. STUPAK. Give me a month. Do you know a month?

Mr. BROWNE. I believe it was November 1997.

Mr. STUPAK. When did you first become aware that the FBI concluded that it had finished its investigation and Wen Ho Lee's clearance should be lifted?

Mr. BROWNE. If you're referring to the remarks that have been reported in the paper by FBI Director Freeh—is that what you're referring to?

Mr. STUPAK. Yes.

Mr. BROWNE. I think I read about those in The Washington Post sometime in like April 1999. I was never directly informed of those.

Mr. STUPAK. No one ever told you?

Mr. BROWNE. No.

Mr. STUPAK. So that was April 1999?

Mr. BROWNE. 1999, whenever that story came out.

Mr. STUPAK. Any idea why you weren't told by the FBI? Did they make attempts to contact you before the stories appeared or anything?

Mr. BROWNE. I certainly had meetings with the people in the local FBI office, but they never raised that issue with me directly. We certainly discussed—the ongoing investigation is the way it was presented to me; it was not present as if there was a change in the status of that case.

Mr. STUPAK. So you knew about the ongoing investigation and the next thing you knew is what Director Freeh had said in the newspaper; correct?

Mr. BROWNE. Correct.

Mr. STUPAK. Okay. Did the FBI—they were requesting a search warrant for Dr. Lee's computer, but they were told that DOE's policy was not too clear, or was not clear about expectations of privacy of lab employees that might have access on a government computer?

Mr. BROWNE. No, it was—my understanding of this is that there was a ruling by the FBI counsel about the adequacy of the approval, that all of our employees signed a waiver, basically, when they became employees, and it was part of our security updates that you signed, saying that "I know that my computer is subject to search by the government, it is government property," et cetera.

My understanding was that when the FBI and the Department of Justice counsel looked at it, they thought that was not adequate unless every day when you signed onto the computer a banner appeared that reminded you of that every day.

Mr. STUPAK. So the FBI made that determination? It wasn't you or your administration personnel there telling the FBI they could not grant access to the computer without a search warrant?

Mr. BROWNE. That's right.

Mr. STUPAK. Did your policies require the FBI to get a search warrant for this?

Mr. BROWNE. No, no.

Mr. STUPAK. Okay.

You said that the FBI—you knew the FBI was doing the investigation, and they were sort of advising you. Were you or any of your people involved—personally involved with this issue, whether it is getting the search warrant or directing the FBI? Or assisting the FBI; I won't say directing.

Mr. BROWNE. When the FBI opens a case, they were responsible for the conduct of that case, and we certainly supported them in all their requests that they made with respect to the investigation. So our people had to help them with access to certain information regarding the individual; and any attempts they were trying to make, they kept us informed about as well. We were in complete communication with both them and the Department of Energy throughout this whole period.

Mr. STUPAK. This was a pretty high-profile case going on, especially as the news stories started to break. Were you personally involved in some of the decisions being made and things like this?

Mr. BROWNE. Up until December 1998, I would say that it was a low-profile case. And it became much more of a high-profile case after December 1998, when we started to obtain our own information in the Department and the FBI obtained more information about the security violations that this individual committed.

Mr. STUPAK. You said that was about December 1998, but if my memory serves me correctly, by then it had taken on a pretty—it had become a high-profile case; even—if my memory serves me correctly, I think even the President was briefed on this by December 1998.

When—were you just sort of out of the loop on this one?

Mr. BROWNE. No, we were not out of the loop. In December 1998, the individual actually passed the polygraph examination and there was a determination at that point to—although he had passed the polygraph, the Department of Energy asked us to re-

move him from his position into a totally isolated part of the laboratory, which we did immediately. And there was a determination at first that it looked like he passed and the case would be basically terminated against the individual.

After a subsequent review of the information, it was determined that he was deceptive on the polygraph and then that led to a much deeper set of investigations.

But we were totally part of the entire interaction. Our counter-intelligence people were involved. It was not like we were out of the loop.

Mr. STUPAK. I guess for a case to get where the President is briefed on it, that has got to be pretty high-profile, and yet I get the impression that you were still giving it low profile until December 1998.

Mr. BROWNE. There was not much evidence up to December 1998 that the FBI was not in a position to prosecute any case, and of course they still have not moved that far against the individual. But the evidence, to my understanding, that I was aware of at that point, they did not have sufficient evidence up until December 1998 to do anything except consider it an ongoing investigation.

Mr. STUPAK. When the President was initially briefed before December 1998, were you or any of your personnel involved in that briefing?

Mr. BROWNE. No.

Mr. STUPAK. Did you prepare any briefing documents for the President or anything?

Mr. BROWNE. No.

Mr. STUPAK. Do you think the lab director should play a role in these investigations?

Mr. BROWNE. I think we—in retrospect, I think we should have had more information provided to us during that period. For example, as I stated, if the information that Director Freeh provided to the Department of Energy had been available, it might have changed some of our viewpoints.

Mr. STUPAK. How much responsibility do you think Los Alamos lab personnel, who handled these requests for computer access and delayed in lifting Dr. Lee's clearance, how much responsibility should you have in that or your personnel?

Mr. BROWNE. We are not responsible for removing the clearance. The Department of Energy's responsible. We can recommend that to the Department of Energy.

Mr. STUPAK. Did you in this case?

Mr. BROWNE. Yes, we did.

Mr. STUPAK. When?

Mr. BROWNE. It was in January 1999.

Mr. STUPAK. On this investigation, did you have a single source person who worked for you, that worked with the FBI and DOE on this?

Mr. BROWNE. That's correct.

Mr. STUPAK. Who was your point person on that?

Mr. BROWNE. It was an individual named Mr. Terry Craig.

Mr. STUPAK. Okay. Thanks.

No further questions at this time.

Mr. UPTON. Thank you.

I'd like to ask Dr. Robinson and Dr. Browne and Dr. Tarter, there was a memo, I guess that DOE was considering. I don't know if they actually drafted it or not, but it was a new contract clause that indicated—would place the lab's annual performance fee at risk if they failed to achieve a satisfactory rating in evaluation of their performance under the security plans.

What is your reaction to that? Is that something that you all could support? Would you agree to forfeit some of the bonus if, in fact, you didn't achieve that type of rating? What is your reaction to that?

Mr. ROBINSON. I think, as a matter of anything, we would make a contract, we would want things to be spelled out as to what the obligations are that you are to meet. We have never favored open-ended contracts, but certainly when reasonable conditions are spelled out, we agree to take those obligations that would be perfectly acceptable. We do that in some other areas.

Mr. UPTON. Dr. Browne?

Mr. BROWNE. Well, our responsibilities for security certainly are at the top priority, along with protection of the health, safety, and environment. In addition, we have a responsibility at all three labs for certifying the safety and reliability of the stockpile each year. So I would think any one of those is paramount to what the government should be evaluating, how well we are doing our job. If any one of those fails badly, then I think one has to have measures in place to ask what caused the failure.

If it is true failure versus something being not quite appropriate, if you see what I am driving at—"marginal" versus totally "unsatisfactory," I think "marginal" many times has deficiencies, and a deficiency doesn't necessarily mean you are failing.

Mr. UPTON. That's right. But you would support some degree of accountability using these bonuses?

Mr. BROWNE. I think it should be graded according to your performance. If you had a graded metric that said, if you are totally "unsatisfactory," that you risk a certain amount of your fee versus if you're "marginal" you risk less, and perhaps if you're "satisfactory," you get a positive indicator on your fee.

Mr. UPTON. Dr. Tarter?

Mr. TARTER. I think my response is very similar to Dr. Browne's. I think there were several responsibilities for each laboratory.

I think safety is an extremely high responsibility. I think security is at the very top of the list; I think certifying the stockpile. And I think, however you decide to apportion those in grading the laboratories, I think those need to have extremely high weight.

And then I think you need to assess in each case the reasons for it, whether they are institutional, whether they are individual, but I think they need to have a way to make a very strong statement a laboratory or the institution does not perform at a satisfactory level in one of those really major areas.

Mr. UPTON. Would all three of you agree that the goalposts, I don't want to say "scenario," but the goalposts memo and work that is being done and laid out has been a very constructive way to meet the ultimate goal of achieving full security within the labs? And have you cooperated fully with regard to that?

Mr. TARTER. Let me just start at the other end with the microphone.

I think—one of the things I think we have asked for very much, and I think—particularly in view of the fact that requirements, particularly in the cyber area, do change very rapidly, I think the goalposts approach and the milestones have a lot of good things. But many of them put you on a plan, you know, how well you are doing as you move along the plan, but also the goal line doesn't shift. And then the next year, you may reevaluate the exact form of the goal line by technology changes and requirements change.

But I think having that each time has been a very, very good thing.

Mr. UPTON. Dr. Browne?

Mr. BROWNE. I would agree with that. I think there's one other point that I think we are all pushing for, having security viewed in an integrated sense with our business much like we've done with safety, so that from the top down to the person, you know, on the lowest level of the laboratory out handling the material sees the whole picture of security integrated with their responsibilities for doing their job. That's how it works for safety.

The goalposts memo is a way to help us get there. The way I see it, it's a very focused opportunity for us to really fix things and then move into this more integrated security management approach.

Mr. UPTON. Dr. Robinson?

Mr. ROBINSON. Yes, as I said in my statement, only doing inspections is not a sufficient route to really get security to the level it needs to be. You have got to take a process to build in the security in all that is done, or you just continue finding things, fixing and finding those.

Preventive activities to try and maintain the security at a higher level is the direction we want to go.

But I think it has been a useful exercise. We do push back if we disagree with particular findings; but others, we say, yes, we see there's a problem, and any time we find a problem in security, you can count on us both to be concerned and to fix it.

Mr. UPTON. Dr. Weigand, you indicated in your testimony that you thought that there were adequate levels of funding throughout this year, I presume you mean calendar year, though maybe it was fiscal, but calendar year to achieve the goals in the goalposts exercise.

Where are we for funding to make sure that that same type of process is continued next year?

Mr. WEIGAND. To achieve the goalposts, I did receive a memo from each one of the directors. It does go across a fiscal year boundary, so—

Mr. UPTON. So it goes into the end of September of next year?

Mr. WEIGAND. I expect their commitment to find the dollars to meet that, meet that level of activity that achieves a "satisfactory."

I will caveat this with one thing, though. My tenure in this position has come during a period of time in which we're trying to work a very challenging nuclear deterrence problem—maintain the safety, reliability, and performance of the nuclear stockpile without nuclear testing. It also is coming under a period of time in which we

have seen several things, like our safety program getting sort of on track, that had been off track; our construction programs getting on track, some of which have been off track; and security getting on track after being off track.

And one of the decisions I made was that I really needed to have a solid infrastructure to build a national program that would serve the deterrence issue. The plant has to be open, the facilities have to be open, they have to be safe, they have to be reliable, they have to be guarded appropriately.

The secrets need to be protected because shutdowns caused by lab lapses in security costs the program grievously. A 2-week shutdown of the system is not a 2-week shutdown. It is 2 weeks of downtime on the computers, another couple of weeks bringing them back up, another couple of weeks getting them loaded with the appropriate data and the researchers back on them. That is very costly to the program.

So I have asked these gentlemen to take the money out of the program because I need the infrastructure. If we continue to do it only on that basis, if we are not allowed to step back and say, what is the impact now of finding that we have increased requirements in security and so forth, we could do harm to the program. And I would not like to see that.

I don't believe we've done harm to the program at this point in time.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Dr. Robinson, the chairman was asking some questions about the goalposts memo, and you said some of the things you do and "others we push back." what do you mean by "push back"?

Mr. ROBINSON. You, this morning, made a reference about passwords for security and that you would have expected a laboratory like Sandia have to have passwords on security. Indeed, sir, we do; we always have. The narrow finding was a question of whether or not our unclassified—I stress our unclassified; neither our restricted information network nor our third network, our security networks were in question, but our unclassified network. Their investigators had been able to penetrate and find some passwords that appeared to be easily broken, not that we did not have a password system in place.

It's those kinds of things that we try and dig into and use a lot more care in the description of; and if we think a finding is not appropriate, we say they're not appropriate. In the cyber security area there is still room for doubt as to what can be done.

Mr. STUPAK. What do you mean by "push back" then? You just don't do it?

Mr. ROBINSON. No, we debate with them about what is appropriate.

For example, Sandia was the first laboratory to have a fire wall. Our colleagues at Los Alamos had installed a new fire wall and they suggested our fire wall should be changed to be as good as theirs. We said we would not unless we could find a U.S.-built fire wall. And that's the kind of debate I would call "push back."

Mr. STUPAK. How long did it take—

Mr. ROBINSON. In the last 2 months we have been able to find and develop a supplier on our own of a fire wall.

Mr. STUPAK. You don't have a fire wall yet?

Mr. ROBINSON. Of course, we have had a fire wall.

Mr. STUPAK. For how long?

Mr. ROBINSON. We have had a fire wall for 10 years. We have changed it three times in that period. The latest change that was proposed, we pushed back against making another change until we could get a U.S.-built fire wall. And that's the kind of push-back activity—

Mr. STUPAK. Mr. Weigand, is that accurate?

Mr. WEIGAND. I don't disagree with what Dr. Robinson is saying. I can't speak for him, but there are a number of things that we negotiate on.

I would like to see us only negotiate on time. We don't negotiate on policy with the laboratories. The policy is very clear. It is sometimes the implementation of the policy that is not. And I don't want to get to wild examples, but in certain select areas, passwords may not have been on every single system at one given time. This may have been a small section of a restricted area.

But the policy is very clear on passwords today and the policy is very clear on understanding how we implement passwords, and I think the laboratories are implementing the policy.

Mr. STUPAK. I think today the policy is very clear on passwords, but it hasn't been in the past.

Mr. WEIGAND. That may very well be true. I can't comment too extensively on the policy of the past.

Mr. STUPAK. Dr. Robinson, other than passwords, is there anything else you would push back?

Mr. ROBINSON. There is one other set of discussions and this involves a particular type of storage repository for classified data, and here there was a difference between two parts of the Department of Energy over what was acceptable and what was not acceptable. And those, we suggest, need to be resolved before we can act on them as to what is an acceptable repository and what is not.

Mr. STUPAK. Ms. Stone, I know you do a lot of these investigations for Mr. Podonsky. Would you agree with that on passwords and on the storage classification and unclassification?

Ms. STONE. What specifically are you asking me about, the push-back?

Mr. STUPAK. The push-back.

Ms. STONE. Sometimes we do encounter push-back during our inspections. From an inspection perspective, it is important that we collect the information and validate the facts. Our validation process is very rigorous where we sit down with points of contact—let's say we were inspecting one of the laboratories, it would be the laboratory representatives, the operations office representatives, and sometimes even Dr. Weigand's folks from defense programs would be out observing an inspection activity.

But it's important for us to be able to present our case and show the facts. And then whether there is push-back or not, provided we are correct on our facts, we move forward with that finding.

Mr. STUPAK. After you present your case, do they ever refuse to carry out the recommendation?

Ms. STONE. We have not, during the period of time since we have worked for the Secretary, had the case where they have said—

Mr. STUPAK. Right, prior to that time. This is all new that the Secretary put in prior to that?

Ms. STONE. Before we worked for the Secretary, beginning in May of this year, many times. There were times where—for example, the classified parts finding that we talked a lot about this morning was one that had not been resolved.

Mr. STUPAK. Okay. Well, let me ask all of you then, do you think the directives by the Secretary, Secretary Richardson, reviewed by Mr. Podonsky, and the integrated security management system set up by Mr. Weigand have improved security at your labs, Dr. Robinson?

Mr. ROBINSON. I believe they have, yes.

Mr. STUPAK. How about you, Dr. Tarter.

Mr. TARTER. Yes.

Mr. STUPAK. Dr. Browne?

Mr. BROWNE. Yes.

Mr. STUPAK. Would it be fair to say, based upon past history, that these steps were long overdue at the weapons laboratory?

Mr. ROBINSON. I would prefer to say that security has had highs and lows over time, as I believe any human activity does. A lot of it is change in focus. I believe during the nineties, as I said in my written statement, the focus was not on security in the early part of the nineties following the cold war. It was very much on will there still be a nuclear weapons program? What will we be able to afford as the budget was reduced in half?

Those activities came higher and, yes, there were some lapses in focus on security during that time. So we are not always at 100 percent, though certainly our desire is to be there.

Mr. STUPAK. So it is fair to say, then, these steps were probably overdue then, right? No?

Mr. ROBINSON. I certainly am not opposed to them at all.

Mr. STUPAK. Okay. Ms. Stone, do you think they were overdue, the steps integrated by Secretary Richardson? I mean, you do the investigations, right?

Ms. STONE. Yes.

Mr. STUPAK. Okay. Dr. Browne, did you and the University of California favor the creation of the new Nuclear Security Administration within the Department of Energy?

Mr. BROWNE. We did not take a position on it. Since we are a contractor to the government, our opinion was that that would be decided and we would abide by the law.

Mr. STUPAK. Well, did anyone from the University of California ever contact Members of Congress about this reorganization?

Mr. BROWNE. Not to my knowledge.

Mr. STUPAK. No? No. Under this new agency, there will be no independent oversight of laboratory security or health and safety in environmental programs. Mr. Podonsky's group won't be looking at your security; nor will General Habiger. Mr. Weigand won't have any authority to make changes or run his integrated security management group.

Nothing this committee has ever seen indicates that the laboratories will be responsive on any of these issues regarding the

strong and continuing oversight from DOE. Even then the labs have managed to avoid making changes until forced to do so by some crisis.

Who do you think will play this role in this new agency of enforcing to make sure that changes are being made?

Mr. BROWNE. I think we don't know how this is going to be implemented yet. We haven't seen an implementation plan.

I believe, if my two colleagues would probably not disagree with this, our expectation is that there would continue to be independent oversight. We don't see that as a problem. We think that Mr. Podonsky's function is a very valuable function for both us and the government.

Mr. ROBINSON. I would respond that there is a much larger history that we haven't discussed of steps the laboratories take to improve security, safety, all of our work, without being forced to do so. But I think there has been no decision as to how oversight would be done by the new agency. At least it hasn't been communicated to me.

Mr. STUPAK. Can you provide us those things you have done without oversight as far as security and safety? I would really be interested in seeing that.

Mr. ROBINSON. How many would you like? It is likely to be a very large volume.

Mr. STUPAK. Well, I can go all the way back to 1978 and start bringing in documentation when Mr. Dingell chaired the Commerce Committee about all the pressure we had to put on the labs to try to tighten security. Even during the heightened investigation we have here, there were letters from Democrats and Republicans on both sides of this, trying to ask and trying to get you to just do what the GAO would recommend, and they weren't done. I don't know if there was a pushback attitude or whatever happened, but it just never happened. And then we have this major incident here in the last year. And quite frankly, when we sit on this side of the bench, we don't know who to trust to do anything on their own, if the labs are going to do it properly.

There is this culture out there and there is no accountability and responsibility and we are very concerned about it. So I would be happy to see your list and I will be happy to provide mine.

Mr. UPTON. Thank you. Mr. Cox.

Mr. COX. Thank you.

Earlier I asked our DOE witnesses whether they wanted to register an objection to what the President's Foreign Intelligence Advisory Board said.

They described DOE as a place with "a dysfunctional management structure and a culture that only occasionally gave proper credence to the need for rigorous security and counterintelligence programs at the weapons labs."

Does anybody on this panel want to register a disagreement with that statement? Dr. Robinson?

Mr. ROBINSON. I think there have been serious problems in the Department of Energy management. We have communicated those to past Secretaries. Basically, when everyone is in charge no one is in charge, and there was not an effective structure within the

Department to bring differences of opinion within the Department itself to resolution.

And sitting where we were as laboratories, we seem to be blowing with the winds of dispute between different parts of the Department on any given day.

I believe that is consistent with the studies of the Galvin report and not out of step with the report of the Rudman Commission.

Mr. COX. The Rudman Commission, the President's Foreign Intelligence Advisory Board, also described the laboratories as possessing science at its best and security at its worst.

Does anybody want to register an objection to that characterization? That was, in fact, as you know, on the cover of their report.

Mr. TARTER. I think we could have a long discussion about aspects of that. I think—I think there are—as you have heard, I think there are a number of security issues. I think—some of the serious ones, I think, are still being, as the Rudman report captured, the actual magnitude of some of the possible security losses are still trying to be understood.

I think the part I would disagree with, to the degree a single phrase captures it, I do not think, and I said that before this committee previously, that the vast majority of laboratory employees—and I can't give you a number of whether it is 95 percent or 99 percent of those who had access to national security data—I do not think—I think that personal security with which they guarded the information they had, I think they always considered one of their highest responsibilities. And so I think to the degree it captured a system characterization, we could debate that. To the degree it captured the opinion and perspective of the employees, I do not think it was an accurate characterization of how employees felt about guarding the security of the information they had.

Mr. COX. So you would prefer that we took this as a failure of management rather than of the employees?

Mr. TARTER. Yes, sir.

Mr. COX. I think we have the right witnesses.

Mr. BROWNE. I would agree with that, Mr. Cox, because the people—remember, the ones that were being colored with this same brush are the people that created the information that we are protecting. If anyone is going to really want to protect it, it is the people who create it. That was a real blow to them that they were being accused essentially of not caring about the information that they had devoted their lives to creating to help our country. That was really very damaging to morale.

Mr. COX. Now, on the preceding panel, Mr. Podonsky described to us the continuing problems at the laboratories with the protection of classified weapons parts.

He mentioned that at Los Alamos he brought this to the attention of the laboratory in 1994; that Los Alamos received clear direction to fix this problem again in 1995 from both the Department of Energy and its field office in that year; again in 1996; and that in 1997, when he, Mr. Podonsky returned to review the progress that had been made on fixing security problems with classified weapons parts, he found that the situation, quote, remains essentially unchanged since 1994.

Why are we here today with these same problems, hearing that now the problem is going to be fixed?

Mr. BROWNE. Well, the problem is fixed today.

Mr. COX. The previous panel, as you were here and listened to, said it was not fixed.

Mr. BROWNE. Mr. Podonsky said it is fixed. We got a satisfactory in the protection of our classified parts at Los Alamos.

Mr. COX. Well, when I asked him that question this morning, he said that in particular where it came to the inventory of parts, that it was on the way to being fixed but it was not fixed.

Mr. BROWNE. I believe we did receive a satisfactory rating on the protection of classified parts.

Mr. COX. You were here for that testimony, were you not?

Mr. BROWNE. Yes.

Mr. COX. Am I not correct that that is what Mr. Podonsky told me this morning under oath?

Mr. BROWNE. I don't remember the details of what he said. Maybe Ms. Stone could clarify that statement. But I thought when he was talking about classified parts at Los Alamos that it was a progress in the past. We made significant improvements and were judged by the most recent audit to be satisfactory. That doesn't mean there aren't areas for improvement. I certainly agree that there are areas for improvement.

Mr. COX. Let's let the record speak for itself on the respective representations of Dr. Browne as the head of the lab and Mr. Podonsky as the inspector.

Mr. BROWNE. Okay.

Ms. STONE. May I interrupt?

Mr. COX. Sure.

Ms. STONE. I work for Glenn Podonsky. Just to clarify Glenn's point on this, one of the things that we have to remember about these fixes to these problems is that many of the sites are implementing what they call compensatory measures. The compensatory measures are normally a very resource-intensive and very high-cost, short-term fix, kind of a Band-Aid that's put on things while you work to a longer-term solution for the problem.

I think we are getting into somewhat of a difference in terminology where, yes, we found the program to be satisfactory but there still remains some things to be done before those longer-term items are actually fully implemented.

Mr. BROWNE. The longer-term items would require line item construction of vaults and vaulted rooms, and those that are multiyear-type of activities. In the meantime, we have increased the number of protective forces by about 25 percent, and we have increased the time frequency of patrols to make sure this material is guarded appropriately. It is behind a fence and it is locked in buildings. It is just not vaulted buildings like you would prefer to have for such parts.

Mr. COX. So stipulating, if we might, to the essential accuracy of what Ms. Stone has just told us, and if that bridges the gap between Mr. Podonsky and yourself—

Mr. BROWNE. Correct.

Mr. COX. [continuing] as to where we are today in October 1999, why did it take until now, inasmuch as this iterative process had

Mr. Podonsky personally going back to Los Alamos between 1994 and 1997 on an annual basis and finding nothing happened?

Mr. BROWNE. Although I wasn't in charge until—

Mr. COX. I know you have only been there 2 years.

Mr. BROWNE. Let me tell you what I know about the period; what I understand, what I have been told, is there were within the Department disagreements about how best to fix this.

Mr. Podonsky is an oversight function. He makes excellent recommendations on how to improve things. Those resources that have to be applied to the problem sometimes—and I think this was in this case a discussion within the Department about how best to solve this problem. Now, you might ask the question, why didn't Los Alamos just go out and fix it? Because we have been asked that question many times during this hearing. And when you are talking about millions of dollars of commitment of resources, we really believe it is important for a contractor like ourselves to have some direct guidance from the government to spend that level of resources.

We are talking about \$2.5 million or \$3 million a year just in incremental costs for the protective forces. So during that time period it is my understanding that there was a lack of agreement on how best to fix the problems that were identified by Mr. Podonsky.

Mr. COX. Dr. Robinson, you look as if you want to respond also.

Mr. ROBINSON. The characterization of security at its worst is a broad statement and covers a lot of areas. I would not agree that all of our security would fit such a categorization.

I am confident some of the areas of our security are, at its best, not only best in DOE but against any other part of the government. And so I think you have to be careful to dissect exactly what is being discussed. With the area of these investigations, our philosophy in security has always been a layered set of protections; that if one area fails, you now have additional areas that would serve as protection and you are trying to stack them up so that you never get a case of all systems failing.

And when we are judged, the things that are reported are problems in a particular layer, not a failure of all of the layers, and that's very important to focus on.

Mr. COX. Dr. Tarter, I wonder if I might ask you about the earlier testimony that we had from Mr. Podonsky concerning the reduction almost by half in the guard force at Superblock.

Mr. TARTER. Right. If I need to get precise dates, I either would like to do them for the record or from the people in back of me, and Dr. Turner might wish to comment on this also, but during a period in the nineties, and again I am not going to be—let me go ahead and do the statement and then—

Mr. COX. Well, at least according to Mr. Podonsky, from 1995—

Mr. TARTER. That's correct.

Mr. COX. [continuing] to 1997, the guard force for—

Mr. TARTER. Was reduced.

Mr. COX. [continuing] for Superblock was reduced by almost half?

Mr. TARTER. Let me give the general sense and then perhaps the—one of the things we did with the agreement at the time, at least of the Department of Energy operations offices, was to use local law enforcement as a surge force to handle much of the spe-

cial response team actions, and that was driven by the fact that we thought we could do the job and we reached an agreement to do the job at a reduced cost by bringing in, in our particular area, the Alameda County Sheriff's Department who were trained with us to do the response.

So we believed that that was the appropriate way to meet the threat, as we understood it, to the Superblock at that time.

We also, I think, and again I need more details from the people in direct charge, but I think we kept the security high at the Superblock and we balanced the area with people in the local law enforcement, again in a surge capacity in the case of an incident.

Much of the addition has been—recently has been that, in fact, it was viewed as no longer an adequate response set of measures and therefore we began some time ago to rehire our own special response team personnel to make them always there onsite. Dr. Turner.

Mr. COX. Is that because the threat has changed between now and 1997?

Mr. TURNER. Could I just add, I think it is because the Department strategy has changed. The point is that in the 1995/1996 timeframe, the Department's strategy was containment. And so in that, using the available forces onsite, as well as the local law enforcement, we were able to accomplish that mission.

Then the strategy changed to recapture recovery. And so we had to—so that—you know, what was sufficient for a containment strategy was now not sufficient for the new strategy of recapture recovery.

Subsequently, the strategy has now changed to denial, which again has, you know—as the strategy changes, then your force structure, your composition, how they are deployed, your time lines, all of those things change.

So the laboratory has been working, you know, to accommodate those changes and bringing on—now they have brought on significant numbers of new guards. There is going to be another class that's going to be completed in December.

I think the point—you know, that's—you are only getting half the story when you get the raw numbers. Those raw numbers—

Mr. COX. Just to make sure that we all understand on the panel, if you go from containment to recapture to denial, you are steadily increasing your security; is that right?

Mr. TURNER. Absolutely.

Mr. COX. So what you are saying is that our standards in 1999 are higher than our standards were in 1997?

Mr. TURNER. Absolutely. So that the numbers of people—

Mr. COX. Why is that? Is that because the real world threat is different in 1999 than it was in 1997? What we are talking about at Superblock is protecting the actual nuclear materials, right?

Mr. TURNER. Yes.

Mr. COX. So this is the most significant security function you have got?

Mr. TURNER. Yes.

Mr. COX. Do we think that the nuclear materials are subject to different levels of threat in 1999 than they were in 1997?

Mr. TURNER. Well, frankly, you know, we don't participate directly in developing the design basis threat.

Mr. COX. All right. So somebody around here, we don't know who, is changing their assessment of just how much security we need for the nuclear weapons material and it was higher in 1995 than it was in 1997 and now it is higher in 1999 than it was in 1997.

Mr. TURNER. Okay. It was higher in 1997 than it was in 1995, and it is higher again in 1999.

Mr. COX. No, no, no, no, that's not what we heard this morning. What we heard was that between 1995 and 1997, we actually reduced significantly the guard force.

Mr. TURNER. Because the strategy then was containment.

Mr. COX. I understand. We had a different strategy, but we also had less security.

Mr. TURNER. We had—we had adequate security to meet that strategy, to meet that threat. And then as the threat and the strategy—

Mr. COX. The threat is a constant?

Mr. TURNER. No, the threat is not a constant.

Mr. TARTER. Let me give you an example, sir.

Mr. COX. I invited somebody to tell me that the threat was different in 1997 than 1999. Was the threat different in 1997 than 1999?

Mr. ROBINSON. Yes.

Mr. COX. Why?

Mr. ROBINSON. But we need to give you a classified answer.

Mr. COX. All right. Let's do it.

Mr. UPTON. We have to vote on it.

Mr. COX. Didn't we vote earlier that we could now go on to classified?

Mr. UPTON. We did not have 10 members here so we did not do that.

Mr. COX. I see.

Mr. UPTON. We could get it in writing.

Mr. TARTER. This is not—the direct answer to your question, as Paul said, we would have to do that in a closed session. But I think General Habiger this morning mentioned an issue which he perceived to be a changing threat for the future, which we have not yet—

Mr. COX. I understand that.

Mr. TARTER. But the chemical and biological issues, I think, are new and whether we put personnel in place to train personnel in those responses, I think, is an ongoing issue, and that is a change.

Mr. TURNER. I think, too, I think it is important to recognize that in security you have an adversary that grows stronger every day, and so your capability cannot just be static.

Mr. COX. Well, that's why I am particularly interested in the diminution, the reduction in the force between 1995 and 1997. The guard force was cut by almost half.

Ms. Stone, do you want to comment on this?

Ms. STONE. The design basis threat is a classified document, but is reassessed on an annual basis. From an independent oversight perspective, we see the changes in the strategy really being driven

by the changes in material inside those areas as opposed—relying more significantly than the changes to the threat.

Yes, there have been some changes in the threat from year to year, but our perspective is that it is the actual, you know, either movement of material from one site to another that really drive those significant changes in strategy.

Mr. COX. Now, when I asked Mr. Podonsky earlier in the day whether he thought that it was wise to make the changes between 1995 and 1997 that were made, he said, no, he didn't think it was wise at all.

Is that your sense as well?

Ms. STONE. Yes.

Mr. COX. And why?

Ms. STONE. To be able to put that much reliance on local law enforcement that really has a limited understanding of DOE, that has a limited amount of abilities, is really expecting a lot of these people that do not have responsibility for the material themselves.

Mr. COX. But now what we saw in the foreign launch situation was that the Department of Defense, not the Department of Energy, decided to rely upon rent-a-cops, as it happened, private security guards that were hired not by the Department of Defense but by the private commercial satellite manufacturers, who told us in our congressional investigations that security was—one of them said security was ninth on our list of priorities.

So we had Pinkerton guards providing what turned out to be wholly inadequate coverage of our national security mission, and here we are relying upon the Alameda County Sheriff's Department compensate for the diminution in the guard force after 1995.

Isn't that essentially what we are talking about?

Ms. STONE. Right. It wasn't solely relying on the Alameda County Sheriff's Department; it was supplemented by. So there were still some number.

Mr. COX. Did the sheriff's department move people over to the labs?

Ms. STONE. No.

Mr. TURNER. No, but they were—

Mr. COX. How long would it take them to get there?

Mr. MORTENSEN. May I answer that?

Mr. COX. Let me ask Ms. Stone.

Ms. STONE. It took more time than I think folks imagined for them to get there, or had hoped for them to get there, and that's probably all I should really say in this forum.

Mr. COX. All right. Well, I do think we need to get answers in another setting.

Dr. Turner.

Mr. TURNER. Could I just add, how this unfolded was that there was some concern about whether the—first of all, this is a swat team from the Alameda County Sheriff's so this isn't just any old—I mean, these aren't traffic cops or people behind a desk. And there was some concern about whether they could meet the time lines or not. And so what was agreed to by Defense Programs, by the field and by headquarters, was that we would run some performance tests back in the 1997 timeframe and we would live by the results of those tests.

As a result of those performance tests, it was agreed that as—you know, with the new strategy and with the response times that the swat team could answer, that it was not adequate; and we moved immediately to, again, abide by the commitment to—to abide by those results and move immediately to hire more guards.

Mr. COX. All right. I think the lights are off altogether, so I don't know whether I have a green light or a red light or an amber light, but I am getting the sense that I am stretching the limits of goodwill here from the chairman to continue asking questions.

What I asked the earlier panel is whether or not they would be willing to provide responses to the committee's follow-up questions, and I hope that we will be able to do that as well, Mr. Chairman.

Mr. UPTON. We will.

Mr. COX. Let me just say in conclusion—because we have had a chance in other fora to, most of us, to talk about these issues before—that I think you are right as leaders of your organizations to parse out the responsibilities of management on the one hand and the employees of the labs on the other hand.

I don't think there is any question at all that we have the best and the brightest at our labs. We want to keep recruiting them and we want to continue to retain them. And I think everybody in Congress, on both sides of the aisle, counts themselves as fans of the laboratories and their important national security and other national missions.

So what we are trying to do here is necessarily accomplish our security objective at the same time as we try to keep people happy in the organization, because security is a central function, if not the central function of our national laboratories.

It is unfortunate that over a period of so many years, these questions have not only gone unaddressed but in some cases have proliferated, and we have more problems rather than fewer; and it is especially unfortunate that as you sit here today and tell us that things are going to be okay, and we have every reason to believe you and we want to believe you, that we have a track record of people telling us in the past that things were going to be okay when they turned out not to be.

So there's a credibility problem for the Department of Energy and derivatively for the laboratories that we have to deal with. And I think that to the extent that management takes this on its own shoulders and says that, maybe in Dr. Browne's case, "I wasn't there but it is still my responsibility," but for everybody else here, "We were there and things should not have been run this way and we are going to change it because it is unacceptable," I think that will give us a high level of confidence.

We know that you need to be defensive about attacks on the laboratories' integrity, but Congress isn't interested in attacking the integrity of the laboratories. We are interested in ensuring that there is security at the laboratories. And I think when we listen to Ed Curran or when we hear General Habiger tell us this morning that you all received an appropriate wake-up call this past year with the uncovering of internal security problems in the publication of both the Cox and Rudman reports, and when he says that your Department of Energy has an historical track record of security deficiencies, for that purpose the labs have to own up to the fact that

you are all part of the Department of Energy, too. And I understand that if we reorganize the Department of Energy and get security as a central focus, an exclusive focus in a new NNSA, that that might make your jobs easier and make your life better and that the dysfunction within DOE itself, external to the labs, has made your jobs unnecessarily difficult in the past.

It is also true, though, that you are very important national leaders and so we look to you folks to fix these problems directly, even if DOE is actually in your way, as has obviously been the case many times in the past.

So we are on your side. We are trying to make sure the job gets done, because it hasn't been done in the past, and we certainly hope we are not back here again next year.

Thanks, Mr. Chairman.

Mr. UPTON. Thank you, Mr. Cox.

I want to say we appreciate your work, particularly as co-chair with Mr. Dicks, on bringing this to light. This is not an easy topic, and for most of us it doesn't involve things in our own district. We don't have a background in this.

Mr. Stupak, I know, does have a law enforcement background, but this is new ground for a lot of us, and we appreciate your testimony. We appreciate your commitment. We want to make sure, absolutely sure, that the comfort level that all of us on this committee have is that your job—that you have not only the sufficient resources but you are doing the necessary job to make sure that these labs are run well and they are secure, and we appreciate the members that were here present. We will probably send some questions on to you for you to respond to.

We also appreciate the staff that have walked us through a number of questions and have done their homework. This is an issue that is not going to go away and we want to make sure, though the horse may be out of the barn in some cases, we want to make sure that that door is locked and it will not happen again.

For that reason, I think the chances are pretty likely that we will see a delegation from this subcommittee visit some of your labs early next year, and we appreciate the assistance and constructive views that you have had and look forward to that as the days unfold.

So with that, this hearing is adjourned. Thank you very much.

[Whereupon, at 2:40 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

g:\graphics\61036.025

g:\graphics\61036.026

g:\graphics\61036.027

g:\graphics\61036.028

g:\graphics\61036.029

g:\graphics\61036.030

g:\graphics\61036.031

g:\graphics\61036.032

g:\graphics\61036.033

g:\graphics\61036.034

g:\graphics\61036.035

g:\graphics\61036.036

g:\graphics\61036.037

g:\graphics\61036.038

g:\graphics\61036.039

g:\graphics\61036.040

g:\graphics\61036.041

g:\graphics\61036.042

g:\graphics\61036.043

g:\graphics\61036.044

g:\graphics\61036.045

g:\graphics\61036.046

g:\graphics\61036.047

g:\graphics\61036.048

g:\graphics\61036.049

g:\graphics\61036.050

g:\graphics\61036.051

g:\graphics\61036.052

g:\graphics\61036.053

g:\graphics\61036.054

Department of Energy
FY 2000
Office of Security & Emergency Operations
(\$ in thousands)

	FY 2000 Request	FY 2000 Amendment	FY 2000 Appro.	Amendment Shortfall
Nuclear Safeguards and Security Program received \$10.0 million increase of which \$3.0 million was earmarked and \$7.0 million was applied to cyber security.	\$ 59,100	\$ 76,100	\$62,100	\$-17,000*
Security Investigations.....	30,000	33,000	33,000	0
Emergency Management.....	98,600	98,600	98,600	0
Cyber Security				
Training (includes education and awareness).....	0	5,500	2,000	-3,500*
Operations such as: CIAC; cyber security hardware and software, research and development, policy and planning	0	29,500	5,000	-24,500*
Total Cyber Security.....	0	35,000	7,000	-28,000*
Program Direction	95,664	105,878	93,652	-10,214
Salaries and benefits; support services, WCF, and other contractual services to support the new organization -- Office of Director & Res. Mgmt -- Foreign Visits and Assignments -- Plutonium, Uran & Spec Nuc Mtl -- Chief Information Officer -- Critical Infrastructure				
Grand Total	283,364	348,578	294,352	-55,214*

*Nuclear Safeguards and Security program requested \$59.1M plus \$17.0M in the amendment (\$12.0M for WMD and \$5.0M to fully arm Headquarters protective force, and additional Headquarters security upgrades.) The Program received an increase of \$10.0M of which \$3.0M was earmarked by Congress. The remaining \$7.0M is being applied to the cyber security request of \$35.0M leaving a shortfall of \$28.0M.

10/21/99

A 12: The testimony was specifically dealing with highly-enriched uranium (HEU) accountability issues related to a portion of Lawrence Livermore National Laboratory (LLNL) HEU inventory. The Department is confident that the discrepancies in inventory values at LLNL are not caused by actual losses of nuclear material but, instead, are caused by measurement errors. A known source of these errors is the inability to accurately measure these materials (HEU). In the past, LLNL's inability to accurately measure portions of their inventory has been due to a lack of new measurement technologies and measurement standards. Recently, LLNL has acquired new technologies and measurement standards for use in their inventory program. With these new capabilities, LLNL and the responsible DOE offices are committed to performing all required measurements related to their nuclear material inventory.

Q. 13: During the hearing, the issue of Livermore's reliance several years ago on the Alameda County Sheriff Department for certain aspects of security— since revoked—was discussed in some length. What, if any, similar security arrangements do the other weapon labs or other DOE sites have with local law enforcement now?

A. 13: I would like to clarify the role that the Alameda County Sheriff Department was to play in the security at Livermore. There was a decision by Livermore to phase-out the DOE Special Response Team (SRT) in favor of using the Alameda County Sheriff Department assets. Under existing DOE policy there are provisions to permit this action. However, the costs associated with security clearances, training, and other certification actions made the approach prohibitive. No DOE facility uses local law enforcement for the protection of DOE assets including Livermore which has re-instituted its SRT capabilities. The arrangements that are in place with local law enforcement, through Memoranda of Agreement, range from providing explosives detection dogs to establishing roadblocks and pursuit operations.

Q. 14: Please provide a comprehensive and detailed list of your as-yet-unfunded budget amendments for FY 2000.

A. 14: The attached data was submitted on October 27, 1999.

Q. 15: During the hearing, you indicated that a new computer password policy would be issued by your office within 10 days. Please provide a copy of that new policy for the record.

A. 15: The recently issued Department "Policy on Password Generation, Protection, and Use", DOE N 205.3, and the associated Password Policy Guide, DOE G 205.3-1 are attached.

U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 205.3

Approved: 11-23-99
 Expires: 7-1-00

SUBJECT: PASSWORD GENERATION, PROTECTION, AND USE

1. **OBJECTIVE.** To establish minimum requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified Department of Energy (DOE) information systems.
2. **CANCELLATION.** DOE M 471.2-2, Chapter VI, Paragraphs 4j(2), and 4j(6); also Chapter VII, Paragraph 12a(2)(a). All remaining provisions of DOE M 471.2-2 remain in effect.
3. **APPLICABILITY.**
 - a. This Notice applies to all DOE elements requiring access to classified and unclassified DOE information systems.
 - b. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements to be applied to DOE contractor and sub-contractor organizations requiring access to classified and unclassified DOE information systems.
4. **REQUIREMENTS.**
 - a. All classified and unclassified DOE multi-user information systems, desktops, and laptops—excluding Personal Digital Assistants (e.g., “Palm Pilots”) and those information systems intended to provide unrestricted public access (e.g., public web servers)—must have and use a password mechanism that authenticates the identity of each person accessing the DOE information system. DOE organizations operating classified information systems shall continue to use automatic password generation software as required by DOE M 471.2-2, Chapter VI, Paragraph 4j(3).
 - b. DOE site managers and Lead Program Secretarial Officers (LPSOs) must designate an individual for each DOE organization who is responsible for the implementation of this policy.
 - c. Each DOE organization must develop, implement, and document in its computer security program plan (CSPP) a password policy commensurate with the level of

DISTRIBUTION:
 All Departmental Elements

INITIATED BY:
 Office of Security
 and Emergency Operations

security required for the organization's environment and specific needs. DOE organizations must address the guidance provided in DOE G 205.3-1 and issue clear instructions to their users regarding password standards. Deviations from DOE G 205.3-1 must be documented in an organization's CSPP.

- d. All DOE organizations are required to have a plan to eliminate the use of clear text reusable passwords, and they must include this plan, with schedule and milestones, in their respective CSPPs.
6. CONTACT. Questions concerning this Notice should be addressed to the Office of the Chief Information Officer, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:



DS
DAVID M. KLAUS
DIRECTOR OF MANAGEMENT
AND ADMINISTRATION

**CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 205.3, PASSWORD GENERATION, PROTECTION, AND USE**

The contractor is required to ensure that the following actions and directions are implemented and complied with to the extent technically feasible.

1. Each Department of Energy (DOE) contractor must ensure that all classified and unclassified DOE multi-user information systems, desktops, and laptops under its purview—excluding Personal Digital Assistants (e.g., “Palm Pilots”) and those information systems intended to provide unrestricted public access (e.g., public web servers)—have and use a password mechanism that authenticates the identity of each person accessing the DOE information system.
2. Each DOE contractor operating classified information systems shall continue to use automatic password generation software as required by DOE M 471.2-2, Chapter VI, Paragraph 4j(3).
3. Each DOE contractor must designate an individual to be responsible for implementation of this policy.
4. Each DOE contractor must develop, implement, and document in its computer security program plan (CSPP) a password policy commensurate with the level of security required for the organization’s environment and specific needs. DOE contractors must follow the guidance provided in DOE G 205.3-1, PASSWORD GUIDE, and issue clear instructions to their users regarding password standards. Deviations from DOE G 205.3-1 must be documented in an organization’s CSPP.
5. Each DOE contractor is required to have a plan to eliminate the use of clear-text reusable passwords, and they must include this plan with schedule and milestones in their respective CSPPs.

DEFINITIONS

Multi-user System. A system that under normal operations has more than one user accessing it simultaneously. Systems accessed by more than one user sequentially (i.e., by one user at a time) without undergoing the necessary procedure to remove residual data between users; are also considered multi-user systems.

Reusable Password. A data item associated with a user ID that remains constant and is used for multiple access requests over some explicit time interval.

Special Character. Any non-alphanumeric character.

PASSWORD GUIDE



U.S. DEPARTMENT OF ENERGY

Distribution:
All Departmental Elements

Initiated By:
Office of Security
and Emergency Operations

PASSWORD GUIDE

1. **PURPOSE.** This Department of Energy (DOE) Guide provides detailed guidance to supplement DOE N 205.3, PASSWORD GENERATION, PROTECTION, AND USE.
2. **SUMMARY.** The security features and procedures detailed below are intended as guidance. It is expected that only those security features or procedures appropriate for a particular environment would be expected to be implemented. Deviations from the guidance provided below and the rationale therefor, however, must be documented in an organization's computer security program plan (CSPP).
3. **REFERENCE.** DOE N 205.3, PASSWORD GENERATION, PROTECTION, AND USE.
4. **CONTACT.** Questions concerning this Guide should be addressed to the Office of the Chief Information Officer, 202-586-0166.
5. **SECURITY FEATURES AND PROCEDURES.**
 - a. **Password Generation/Verification.** If employed, password generation or verification software should ensure that passwords are generated using those security features listed below which would be appropriate for a given site.
 - (1) Passwords contain at least eight non-blank characters.
 - (2) Passwords contain a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions.
 - (3) Passwords contain a nonnumeric in the first and last position.
 - (4) Passwords do not contain the user ID.
 - (5) Passwords do not contain any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); dictionaries for other languages should also be used if justified by risk and cost benefit analysis as documented in the CSPP.
 - (6) Passwords do not employ common names; that is, the password is checked against a set of common names to validate that the password does not contain any of the names, spelled forward or backwards (assuming that the name is over three characters).

- (7) Passwords do not contain any commonly used numbers (e.g., the employee serial number, Social Security number, birth date, phone number) associated with the user of the password.
 - (8) Passwords do not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."
- b. User Selected Passwords. In those cases where the user selects his/her own password (regardless of whether said password is verified by password verification software), the user should ensure that the selected password is consistent with those security features listed below that would be appropriate for a given site.
- (1) Password contains at least eight non-blank characters, provided such passwords are allowed by the operating system or application.
 - (2) Password contains a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions, provided such passwords are allowed by the operating system or application.
 - (3) Password contains a nonnumeric in the first and last position.
 - (4) Password does not contain the user ID.
 - (5) Password does not include the user's own or, to the best of his/her knowledge, close friends—or relatives—names, employee serial number, Social Security number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed.
 - (6) Password does not, to the best of the user's knowledge, include common words that would be in an English dictionary, or from another language with which the user has familiarity.
 - (7) Password does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place.
 - (8) Password does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."
 - (9) Password employed by the user on his/her unclassified systems is different than the passwords employed on his/her classified systems.

- c. Password Protection. Individuals must not –
 - (1) share passwords except in emergency circumstances or when there is an overriding operational necessity, as described in the approved CSPP;
 - (2) leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password;
 - (3) enable applications to retain passwords for subsequent reuse consistent with the organization's CSPP.
- d. Password Changing. Passwords must be changed–
 - (1) at least every 6 months;
 - (2) immediately after sharing;
 - (3) as soon as possible, but within 1 business day after a password has been compromised, or after one suspects that a password has been compromised; and
 - (4) on direction from management.
- e. Administration. If the capability exists in the information system, application, or resource, the system must be configured to ensure the following.
 - (1) Three failed attempts to provide a legitimate password for an access request result in an access lockout that will be automatically restored following a predetermined time period decided by the system manager. Alternative responses (e.g., by increasing the delay between attempts with each failure) to three failures to provide legitimate passwords for an access request (e.g., by increasing the delay between attempts with each failure) are also acceptable assuming such alternate responses are documented in the approved CSPP.
 - (2) When a password specification does not comply with those requirements of 5a and 5b that are implemented, and if the failure to comply is verifiable by automated means, then the password specification is rejected.
 - (3) After 6 months of use, individuals are notified that their passwords have expired and must be changed within five access requests or lockout will occur.

- (4) Any password file or database employed by the information system is protected from access by unauthorized individuals as technically feasible.

BY ORDER OF THE SECRETARY OF ENERGY:



/s/
DAVID M. KLAUS
DIRECTOR OF MANAGEMENT
AND ADMINISTRATION

**OAK Response to Questions for the Record Submitted to Dr. Jim Turner, Manager,
Oakland Operations Hearing of the Subcommittee on Oversight and Investigations
October 26, 1999**

- Q. The Committee understands that, back in 1994-1995, Mr. Podonsky's office reviewed computer security practices and recommended heightened security practices on the unclassified systems, in order to prevent classified information from being improperly transferred to the unclassified systems and to prevent unauthorized users from accessing the unclassified systems. The committee also understands that you and others in the DOE field and lab management offices objected to increased computer security measures at the time, stating that they were not worth the cost and that you would simply accept the risk of poor security.*
- A.** Mr. Podonsky's office conducted a review of LLNL computer security practices in the winter of 1993 and issued a report in April, 1994. The report contained a finding that included a concern that there were insufficient reviews and controls for the transfer of files from classified to unclassified systems. This concern was addressed in the LLNL corrective action plan, which was completed and validated by OAK in August, 1995. When Mr. Podonsky returned to LLNL for a follow up review in July, 1997, he reported that "protection and control measures are well established and appear to be well implemented" and that "these [new file transfer] procedures have been tested, certified, and accredited." It is not clear what the committee is referring to regarding "unauthorized users" because there was no such finding or concern identified in Mr. Podonsky's report; however all of the findings and concerns raised in the report were addressed in the LLNL corrective action plan, closed by LLNL, and validated by OAK. Neither OAK nor LLNL objected to correcting the findings and concerns raised in the report. At no time has OAK been willing to accept "poor security."
- Q. Is it true that you objected back in 1994-1995 to implementing some of the basic computer security measures now being implemented at Livermore and the other labs under orders from DOE Headquarters and as a result of Mr. Podonsky's recent inspection? If So Why?*
- A.** No. Mr. Podonsky made no such recommendations in the 1994 report. The findings and concerns raised by Mr. Podonsky in 1994 were all addressed in the LLNL corrective action plan and the associated corrective actions were completed.
- Q. If you did not object at the time to these recommendations, then why were they never implemented until after the most recent directives from the Secretary and inspections by Mr. Podonsky's office.*
- A.** The measures now being implemented were not recommended in 1994-1995, they are new issues identified in the April/May 1999 inspection at LLNL. These issues are all related to the implementation of the Tri-Lab Action Plan of April 14, 1999 and the Six Further Enhancements to Cyber Security issued by the Secretary on May 11, 1999.

Questions for the Record Submitted to Dr. James Turner, Manager, Oakland Operations Office Hearing of the Subcommittee on Oversight and Investigations October 26, 1999

Q: How is it that your office can conduct annual surveys and have daily contact with the Livermore Site, yet not have identified or corrected the problems that Mr. Podonsky's teams have identified over the years, such as classified parts and other classified information protection and access controls, computer security, and foreign national remote computer access?

A: The Oakland Operations Office (OAK) takes exception to the assumption that OAK has not "...identified or corrected the problems that Mr. Podonsky's teams have identified over the years..." Mr. Podonsky's team was on-site at Lawrence Livermore National Laboratory (LLNL) in 1993. During that inspection they identified issues associated with MC&A (lack of measurement equipment), Personnel Security (Human Reliability Program not broad enough), Classified Matter Protection and Control (Foreign Ownership Control or Influence [FOCI] and Need to Know issues), Classified and Unclassified Computer Security (generic plans, accreditation and configuration management issues), Emergency Management and Protection Program Management (lack of effective follow up).

Prior to this review, OAK had conducted its Annual Survey of LLNL and identified the following issues: Classified Computer Security (processing classified without DOE approval, generic plans and accreditation and configuration management issues), MC&A (procedural deficiencies and issues with corrective action plans) and Protective Forces (training related problems). In addition, OAK's annual Contract Appraisal identified an issue in Protection Program Management (lack of effective follow up) and OAK's Federal Manager's Financial Integrity Act report identified an issue with LLNL's lack of measurement capabilities (these latter two items were identified subsequent to the completion of the '93 survey).

Corrective Action Plans (CAPs) for the OSE and OAK survey findings were required for those issues not closed in "real time"; those CAPs were tracked against their milestones for closure and all have been closed. There are no significant differences between what OAK identified and what was reported by the OSE.

The OSE did not re-visit LLNL until 1997, during which time OAK identified 44 issues/concerns in the following areas: FOCI issues (documentation), Computer Security (network and security plans), MC&A (MC&A plan deficiencies and inventory weaknesses), Self-Assessments (inadequate, not completed), Quality Control /Assurance on documentation (performance tests, training plans), and access control issues. All of these items resulted in CAPs that were tracked against their milestones; all are closed.

The OSE returned in 1997 to conduct a "Site Profile" from which they recommended that OAK/LLNL continue to implement the upgrades identified for the Superblock; complete the in-progress Site Safeguards and Security Plan (SSSP) and continue to identify/characterize all radiological targets. All of these actions have been completed. In addition, the OSE inspection team identified an open storage of classified parts issue that had not been previously identified by OAK; they re-stated their concern over LLNL's inability to measure uranium and they re-stated their concern over OSE's inability to obtain sufficient information on Special Access Programs (SAPs).

The open storage issue is a legitimate "find" by the OSE and LLNL moved quickly to begin correcting the problem. This included a lab-wide assessment that identified several additional facilities with similar open storage problems. A CAP is in place and LLNL is on track towards full resolution of this issue by 12/99. It needs to be noted that although these facilities were not in compliance with DOE Orders, they are within the Limited Area at LLNL and under routine guard checks. It also needs to be emphasized that this issue involves parts, as opposed to full-up components, and not readily identifiable as to purpose/function. In addition, the OSE re-stated their concern about LLNL's inability to measure uranium, an issue which is a complex wide problem. LLNL obtained the measurement equipment in 1998 and spent the next 3 years trying to obtain the measurement standards for the equipment. These standards arrived in October of 1999 and measurement has commenced. Finally, the SAP issue was not an issue that could be resolved by either OAK or LLNL. This issue was resolved at the DOE Headquarters level with the OSE being denied access.

The OAK survey for 1998 identified issues with MC&A (management attention and inventory), FOCI (procedures), Physical Protection (classified parts and Protective Force orders), Information Security (documentation/procedures), and Personnel Security (PSAP related issues). All of these had CAPs and all but one are closed. There was no OSE in 1998.

The OSE inspection for 1999 identified issues associated with protection strategies, documentation of results and assessments, MC&A (non-HRP personnel with access, TID verification, procedures and lack of uranium measurements), issues associated with physical security systems (access, barriers, scenarios), open storage of classified parts (deficiencies in progress, non-GSA repositories), Computer Security (issues associated with the INFOSEC plan, remote dial up access) and issues related to Personnel Security (use of Letters of Interrogatory, reinvestigation submissions). All of these have CAPs; they have either been closed or are on target for closure, most by the end of December, 1999.

The OAK survey for 1999 identified similar issues plus issues associated with the lack of management attention to ensure effective planning, Computer Security (insufficient assurance of properly marked media), and concerns associated with video cameras/sensors and MC&A. All of these have CAPs and are on track for closure.

A review of the issues, findings and concerns identified since 1983 indicates that very few have not been identified by OAK or corrected by LLNL. The classified parts issue was first identified in 1997 and an immediate plan was put into place to correct the deficiencies. An assessment was conducted to identify other facilities with similar problems; corrective actions were developed for those facilities. These facilities, with significant dollar and human resources expended, will be in compliance by 12/99. Computer Security issues are going to occur in a dynamic computing environment. OAK's responsibility is to ensure that LLNL's configuration management plans address all potential issues and are in compliance with DOE policy. OAK has identified numerous issues associated with computer security over the years and has demanded corrective action be taken by LLNL. With regards to foreign nationals having remote computer access, this was a long-standing practice not only at LLNL but around the DOE complex as well. It had never been an issue with any review team, not OSE, not OSS, not GAO, not OAK. This practice was in full compliance with existing DOE policy and became an "issue" as a result of the Wen Ho Lee situation and consequently an area of concern for the inspection team.

The only "issues" that Mr. Podonsky's review team have identified over the years that have been reoccurring are: inventory accounting issues directly related to uranium (a complex wide problem), SAP access (an issue resolved by DOE/HQ) and open storage of classified parts, a legitimate issue that OAK expanded upon and one that will be resolved shortly.

In summary, DOE OAK has identified significant security issues for which corrective actions have been defined, implemented and validated. DOE OAK's continuous on-site presence at LLNL ensures that issues are identified quickly, compensatory measures are initiated and corrective actions/milestones are established. To imply that OAK has done otherwise is simply in error. DOE OAK has identified issues relative to Protective Force performance and training and, as a consequence, has disallowed LLNL's use of a facility until it can be adequately protected and those protection strategies performance tested. DOE OAK identified the MC&A inventory deficiencies at LLNL and has insisted upon "repeatability" of LLNL's ability to perform measurements and resolve inventory differences prior to closing this finding. DOE OAK identified the need for and insisted upon organizational changes to provide better LLNL management awareness of issues/concerns within MC&A. DOE OAK has insisted upon receiving improved protection strategy documentation, self-assessments, configuration management plans, corrective actions and MC&A plans.

Without DOE OAK's on-site, daily oversight, most issues/problems would go unnoticed until an outside team came in to do a review. Furthermore, without DOE OAK's on-site presence, there is no assurance that issues identified by an outside entity would be expeditiously dealt with. DOE OAK and LLNL have taken, and will continue to take, their safeguards and security responsibilities seriously.

**Answers to Questions for the Record Submitted to Dr. Jim Turner,
Manager, Oakland Operations Office Hearing of the Subcommittee
on Oversight and Investigations
October 26, 1999**

Q: In 1998, your office's annual security survey rated Livermore "marginal", yet that same year, your office gave Livermore a "good" or meets expectations in its contract performance evaluation in the security area, presumably adding to the annual performance bonus the lab received under its contract with DOE.

How does such a discrepancy happen, and what message are we sending when we actually reward the lab for marginal security?

A: Lawrence Livermore National Laboratory's (LLNL) contract related safeguards and security performance rating of "good" did not contribute to any performance bonus; LLNL was not rewarded for marginal performance. A rating of "good" results in no support for a bonus increase fee. Any bonus which LLNL received in 1998 came from its science and technology performance and performance in areas other than safeguards and security, which accounted for only 4.5 percent of the total contract evaluation.

In FY 1998, the Oakland Operations Office safeguards and security survey and contract evaluation were complementary assessment tools, which had different purposes. The survey was a comprehensive evaluation looking at all safeguards and security areas. In FY 1998, the survey's Marginal rating of LLNL primarily stemmed from LLNL's problems in the nuclear material control and accountability program. While all other areas were rated satisfactory, the Oakland Operations Office wanted to send a message to LLNL that special attention needed to be placed on nuclear material control and accountability. Even though the Oakland Operations Office survey indicated that all other areas were rated satisfactory overall, the survey identified 16 findings (deficiencies) and five concerns (conditions which would lead to deficiencies) in the areas of protection of classified parts, computer security and personnel security.

In consonance with the Department's contract reform efforts, the Oakland Operations Office FY 1998 contract performance evaluation for safeguards and security primarily focused on a select few performance measures which LLNL happened to do well in. These performance measures were negotiated months before the beginning of the fiscal year and therefore were not as responsive to changing situations. In addition, the intent of the performance measures was to focus on capturing information on a few key performance areas in a way that the survey did not. As it turned out, the selected performance areas' ratings (special nuclear material protection – not accounting and control; LLNL self-assessments and LLNL corrective actions to identified problems) generally matched evaluations in the safeguards and

**Answers to Questions for the Record Submitted to Dr. Jim Turner,
Manager, Oakland Operations Office Hearing of the Subcommittee
on Oversight and Investigations
October 26, 1999**

security survey. But because the performance measures were not as comprehensive as the survey, the evaluation result was different.

To ensure that the problems described above do not happen in the future, DOE and the Oakland Operations Office made changes in the manner in which LLNL is evaluated. Starting in FY 1999, the contract related safeguards and security performance ratings structure has been changed so that they are the same as the standard DOE safeguards and security ratings. Starting in FY 2000, new contract performance measures ensure exact alignment between DOE safeguards and security evaluations and contract performance results.

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
Committee on Commerce, U.S. House of Representatives
Answers for the Record
Dr. John C. Browne, Director, Los Alamos National Laboratory

QUESTION: According to information provided by Los Alamos to the Committee, recent evaluations of protective force deficiencies has led Los Alamos to increase its number of guards by more than 80, or a base of less than 300—about a 35% increase. How did the lab get itself into a position in which you needed such a massive increase in guards just to achieve a satisfactory rating? What steps have you taken to ensure that protective force deficiencies do not reemerge in the future?

LABORATORY RESPONSE: Our past problems with protective force deficiencies were focused on training issues and not the number of guards. For the past several years, Los Alamos has invested a significant amount of resources into ensuring that our security force is the best-trained and best-equipped force possible. Our security training is fully certified. We have increased the training staff and the number of training hours required for every member of the protective force. In addition, we have an in-depth and rigorous performance-testing program that constantly tests the capabilities of our protective force. The results of our efforts are exceptional. For example, over the past two years, 98.5% of the protective force have passed the critical performance tests on the first attempt. Performance is tested in areas of firearms, physical fitness, handcuffing, and unarmed defense techniques.

Los Alamos is confident that this program will continue to prevent a re-occurrence of the concerns raised by the GAO of the early 1990's.

With respect to the increased number of guards, our increased staff was not prompted by poor ratings. Our recent hiring efforts were based upon our planning and analysis results based on DOE scenarios. These results indicated the need to increase the guard force to deal with a postulated increasing threat. Los Alamos maintains a very comprehensive and aggressive analysis and planning program. The goal of this program is to ensure the proper number of guards with the correct weapons mix is available to defend our most sensitive activities.

QUESTION: You noted in your testimony that the lab has taken action to improve protection of classified weapons parts since the inspection by Mr. Podonsky's team. But why did you permit such parts to be stored in unsecured facilities in the first place, and for how long did that situation exist? Did you believe that leaving classified weapons in unsecured facilities, without alarms and without reasonably timely guard checks, met DOE Requirements, or any common sense notion of proper security?

LABORATORY RESPONSE: Los Alamos's classified parts were never stored in "unsecured" facilities. Los Alamos was in compliance with the 1994 DOE orders, which allowed for the storage of classified parts in locked buildings. These buildings were within security areas with guard checks performed on a periodic basis in accordance to the DOE orders. Los Alamos's compliance to the DOE orders was specifically recognized in the 1994 Office of Security Evaluation audit. The 1994 OSE report stated the following:

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
Committee on Commerce, U.S. House of Representatives
Answers for the Record
Dr. John C. Browne, Director, Los Alamos National Laboratory

Page 9: "According to AL and LANL, the Headquarters Office of Safeguards and Security has indicated that the LANL storage practices comply with the minimum DOE security requirements... Because the practices have been interpreted to comply with the minimum requirements, Security Evaluations has raised the policy issues to the Director of National Security and Nonproliferation for consideration and resolution."

Page 24: "Though LANL is meeting minimum DOE requirements... a reexamination of DOE policy is warranted."

It is also important to note that this protection posture was not limited to Los Alamos, but was mirrored at virtually every DOE site with similar inventories of classified parts. The inspection in 1994, by Mr. Podonsky's team, resulted in a concern over the adequacy of DOE's policy for protecting classified parts and began the process of changing those requirements. [Please refer to the next question for additional discussion of the 1994 DOE order and subsequent Laboratory security improvements for classified parts.]

QUESTION: You testified that the long-standing problem with protection of classified weapons parts was unresolved for years because of disagreement within the Department of Energy over how the matter should be resolved. Yet, according to Mr. Podonsky's 1997 report on this matter, the lab was provided clear guidance by both the relevant DOE field office and DOE headquarters back in 1995 and 1996. Do you dispute these statements? What, exactly, was the nature of the alleged disagreement within DOE, and how was it finally resolved? When was the lab provided with, in your opinion, clear guidance on this matter, and from whom did such direction come from? Was there any reason that Los Alamos could not have taken years ago the steps it recently took to reduce this storage problem, such as consolidating and reducing the number of parts and increasing guard checks.

LABORATORY RESPONSE: Los Alamos maintains that the guidance from DOE on this issue was not clear, nor was it timely. DOE internal correspondence from 1995 to 1997 discussed the possible solutions to the policy concerns raised in the 1994 inspection. Los Alamos maintains that this guidance was not officially issued to the field until January 1999. This is supported by the fact that all sites with classified parts in non-standard storage are now adopting the new order and new security requirements.

It is our understanding that the nature of the dispute within DOE was focused on the level of effort required to increase classified parts security. On the one hand there were advocates for requiring the construction of alarmed areas to house the parts, on the other hand there were advocates for simply documenting the protection strategies in official analysis reports. The issue was ultimately resolved by DOE/NN when they published DOE Order 471.2-1B in January 1999. The new order did not mandate any specific security measures (e.g. alarms), but took the approach of conducting vulnerability analyses and having the results approved by the cognizant DOE field office.

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
Committee on Commerce, U.S. House of Representatives
Answers for the Record
Dr. John C. Browne, Director, Los Alamos National Laboratory

It is not accurate to say that Los Alamos did nothing to improve the classified parts situation while we waited for DOE requirements to be published. From the very beginning of this issue in 1994 we have worked to improve security. During this time we reduced the number of parts by getting rid of excess inventory. We are continuing with this effort to this day. We also reduced the number of buildings holding classified parts, added additional guards, and increased the patrol checks of facilities with classified parts. Based on those enhancements, we had submitted a DOE variance for operations during this period. Most importantly, we incorporated these requirements in a line item construction project that was submitted to DOE in 1997. At this point, DOE has decided not to support the classified part storage portion within this line item construction project. The classified part storage portion would correct the classified part concerns noted in the 1997 OSE Site Profile report. Currently, Los Alamos is using manpower to correct this concern at an annual cost of more than \$3M. This same issue could be solved by technology; thereby, substantially reducing the annual recurrent personnel cost.

It is our firm belief that we took the necessary and appropriate steps to improve the security for classified parts while we waited for the DOE to reach their conclusions and issue new instructions.

Question: You issued a memorandum to all Los Alamos employees on June 18, 1999, concerning contacts with Federal and State officials, including members of Congress and their staff. In this memo, you reiterated Los Alamos Policy that employees are not to have any contact with government officials or employees without first getting approval of lab management, and that all such communications must be coordinated through your government relations office. Notably, this memo was issued right after a federal court ruled in favor of one of Los Alamos' most notorious whistle blowers. Were you suggesting, in this memo, that potential whistle blowers risk adverse action for bringing complaints about security, or safety for that matter, to Congress' attention? If this memo was designed to be limited to instances of actual lobbying, why did the memo fail to remind employees of their right and duty to report instances of waste, fraud, abuse, or other illegal or unsafe activities to Congress? Will you issue a correction, reminding employees of their rights and duties in this regard? If not, why not?

Laboratory Response: The June 1999 memorandum was basically a reissue of a long-standing notice against lobbying by Laboratory employees. Essentially the same notice has been issued periodically for many years as a reminder that this activity is forbidden by law and contract. Although we think the intent of the memo, which referred repeatedly to "programs," was clear, we are re-drafting the message to make it clearer that employee whistle blower actions are not subject to Laboratory control.

Question: According to a June 1999 memo from the Energy Secretary, DOE is drafting a new contract clause that would place the labs' performance fee at risk if they fail to achieve a satisfactory rating in an evaluation of their performance under their security plans.

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
Committee on Commerce, U.S. House of Representatives
Answers for the Record
Dr. John C. Browne, Director, Los Alamos National Laboratory

Would you agree to forfeit your lab's performance fee or senior management bonuses if the lab received marginal or unsatisfactory ratings in any security area? And would be willing to have independent inspections determined the ratings, as opposed to the DOE field office annual surveys?

Laboratory Response: We believe that a negotiated, graded scale of reductions against the contract fee for serious performance failures that can be attributed to the contract manager would be a fair and equitable practice. Our performance is measured annually by the University of California and DOE in many areas, such as, mission accomplishments, ES&H, security, business practices, etc. Marginal or unsatisfactory performance in any of these areas should affect the fees in a graded manner.

Question: The Committee understands that each of the labs permits foreign nationals from sensitive countries like China, Iran, Pakistan, and Russia to have authorized user status on their unclassified systems—either on site or via remote dial up, or both. Is that correct with respect to your lab, and if so, what are the actual numbers from each sensitive country?

Laboratory Response: Access to the Lab's internal unclassified computer network by sensitive country foreign nationals can be authorized under certain conditions. The request, similar to the request for physical entry, must be made by a Laboratory host for specific computer resources for definite programmatic purposes. Required approvals include the cognizant Associate Laboratory Director. Access is limited to authorized portions of the internal unclassified network. In this network, subnets are being inventoried for sensitive content and protected with passwords so that additional authorization is needed for entry. Compliance of passwords with our password policy is constantly being checked, as well as net monitoring for break-in attempts and unusual activity. Remote access to the unclassified internal network is subject to all of these constraints and in addition requires using a Laboratory-issued token card (obtained through the same approval process) to generate a one-time password, which invokes "two-factor" authentication: a valid Lab-issued card is being used, and the user has its PIN. Currently about 80 sensitive country foreign nationals hold token cards, including 32 from China, 25 from India, 15 from Russia, and 6 from Taiwan.

Question: Prior to the recent inspection, how did your lab ensure that these Chinese or Russians were not gaining access to information that they don't have any need to know, or are prohibited by law from seeing? Was there anyone monitoring them?

Laboratory Response: Since the early 1980's, all users including foreign nationals of the integrated computing network (ICN) resources have been monitored daily for abnormal behavior. (ICN resources include systems like the supercomputers or mainframes.) The Laboratory Network Anomaly Detection Intrusion reporter builds a computing profile for every ICN user. If a user operates outside this profile, it is flagged for further investigation. An example of such anomaly would be a user who normally works for 8 am to 5 pm. If said user

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
Committee on Commerce, U.S. House of Representatives
Answers for the Record
Dr. John C. Browne, Director, Los Alamos National Laboratory

was to suddenly use the system at 3 am, this action would be flagged as an anomaly. In addition, the Laboratory formed the Security Incident Response Team in late 1996. This team uses some automated and manual monitoring methods to detect cyber vulnerabilities. Upon detection, this team assists with corrective actions. Los Alamos security cooperates closely with the FBI and other government agencies to combat unauthorized access to our computer systems. We also utilize third parties to scan our unclassified environments. These parties have included DOE Office of Security Evaluations, DOE Computer Incident Advisory Capability, Sparta Inc., Engarde Inc., and ISS Inc.

Los Alamos security policy for many years includes a requirement that the line management of the hosting work unit monitor the computer activities of their sensitive country visitors. This includes the managers's right to review the visitor's computer file contents, designate operating system privileges; such as, read, write, program execution, etc., and limit the foreign national's access to only authorized information. Increasingly—before and after the most recent security audits—automatic features are being implemented to limit this access to authorized portions of the unclassified network.

Even though Los Alamos strives to maintain a good cyber security program, events over the last year have emphasized the need for further improvement. Recent cyber security improvements include 100% scanning of all outgoing e-mails, upgrades in our unclassified file scanning, implementing a new DOE/Laboratory cyber security plan, requiring additional employee cyber security awareness training, and implementing the new DOE password policy.

Questions: According to Mr. Podonsky's cyber experts, Los Alamos policy required that background checks be performed on sensitive country foreign nationals before computer access was authorized, but the inspection team could not verify that such checks actually occurred due to insufficient record keeping by Los Alamos. Did the lab actually conduct background checks on these foreign nationals prior to granting them authorization to access the computer systems? If so, please provide the supporting data.

In March 1999, I directed that indices checks are to be part of the screening process for every sensitive country foreign national visitor to Los Alamos. (Prior to this time, we operated under a procedure allowed by the DOE's foreign visitor policy to make the indices check discretionary for visitors to nonsecurity facilities.) The new requirement is included in the Lab's Counter-intelligence Implementation Plan and DOE Notice 1421.1. Documentation of the indices check is kept in the DOE's CARDS database.

Question: What steps have you taken since the recent inspection to tighten controls on such access and implement the new DOE policy on cyber access by foreign nationals?

Laboratory Response: Earlier this year, a long-range plan for cyber security was being developed in coordination with the other DOE-Defense Program laboratories, which, although

October 26, 1999 Hearing of the Subcommittee on Oversight and Investigations
 Committee on Commerce, U.S. House of Representatives
 Answers for the Record
 Dr. John C. Browne, Director, Los Alamos National Laboratory

no longer a formal tri-lab activity, provided a roadmap with much technical detail for meeting the challenge of protecting national security information on our computers in the face of ever-changing threats. This plan provided the basis for most on-going activity, although it will evolve to accommodate new considerations such as evaluations like the August OSE audit and new formal requirements like the November DOE Notice 250.2, *Foreign National Access To DOE Cyber Systems*. Based on groundwork laid earlier, in the last three months we focused on minimizing Yellow (internal unclassified) network vulnerabilities potentially exploitable by insiders. This program watches for unauthorized network modem connections and enforces stronger password protection of the Yellow subnets and subsystems. Presently noncompliance is in the range of one-tenth of one percent, and will be kept near zero by the new practice of disconnecting unauthorized or non-compliant systems.

Question: Mr. Podonsky's team found various computer security vulnerabilities at the labs, such as passwords, firewalls, and transfers from classified to unclassified systems, among others. Most, if not all, of these issues had been raised in earlier inspection reports dating back to 1993 and 1994. Why did your lab fail to address these computer security vulnerabilities for so long, and why did it take the recent inspection and directives from the Secretary to prompt improvements in this area.

Laboratory Response: To the best of my knowledge, all OSE and DOE-AL findings have been corrected. However, we do not find a record of OSE issues relating to passwords, firewalls, and file transfers prior to 1997. Most of our security upgrades result from our own vulnerability assessments and these have resulted in cyber security upgrades for many years. Our approach has always been to tackle the most security-significant issues first. Earlier improvements addressed the classified computing environment, while more recent changes enhanced protection of the "Yellow" internal unclassified network. A few highlights of this graded approach are noted below:

- 1993—isolated ("air-gapped") the classified computing network from the unclassified network.
- 1996—developed the Mercury file transfer process, a process to regulate the transfer of *unclassified* information from classified data storage to unclassified data storage.
- 1998 (March)—implemented configuration control plan for Red network.
- 1998-99—separated the unclassified network into publicly accessible Green network (the Lab's public information web site) and the internal, firewall-protected Yellow network.
- 1998—instituted a Laboratory-wide policy requiring passwords generated by Laboratory-issued token cards for access to many computer network services.
- 1999 (August)—initiated monthly vulnerability scans of our Yellow Network (this has been going on for some time in our Red network) and continuous "war dialer" scans for unauthorized modems
- 1999 (August)—strengthened the Mercury file transfer process by requiring two people to authorize a file copy from the classified system to unclassified, both persons Q-cleared, one person enrolled in PSAP, and review required by an Authorized Derivative Classifier.
- 1999 (September)—implemented three months ahead of the required date, a new password policy similar to DOE's Notice 205.3.

Answers to Questions for the Record
Dr. C. Paul Robinson, Director
Sandia National Laboratories

United States House of Representatives
Committee on Commerce, Subcommittee on Oversight and Investigations
Hearing Held on October 26, 1999

Q1: You stated in your testimony that security was de-emphasized in the mid-1990s, with substantial cutbacks, but problems were not identified until 1998. You attributed that failure to the fact that "compliance was not a reliable indicator of actual performance." Could you explain in greater detail what you mean?

Response:

Compliance with DOE directives on security is essential—but not necessarily sufficient—for effective security.

In the past, our self-assessments and the assessments by DOE focused mainly on compliance to specific requirements in DOE orders rather than actual performance. For example, to save money we cut back on training for our protective force. We believed that if we met the minimum number of hours of training called out in the DOE orders, we were okay. However, actual performance testing of our force showed that after a while, the amount and type of training we were providing was insufficient for them to maintain the level of actual competency in firearms manipulation and accuracy that we feel is essential. We had focused on counting hours rather than actual performance after training.

Another example has to do with protection of classified matter. In one area that was cited by the inspectors from the DOE Office of Independent Oversight and Performance Assurance in July, our security plans met the specific requirements of the then-applicable DOE Manual 5632.1C-1; however, the overall level of protection being provided really wasn't up to the latest standards. Here again, we had focused on compliance rather than continually asking ourselves what the residual risk was and whether or not that risk was acceptable.

Most strikingly, in 1993 we "complied" with a directive from DOE modifying the accountability requirements for all Secret documents. DOE's modified accountability program removed the requirements for unique document numbers and maintenance of accountability records for documents, inventories, destruction certificates, written authorizations to reproduce, and some internal receipting. While this change clearly saved money, it reduced our capability to quickly detect the absence of a document, and it eliminated our ability to monitor the traffic in secret documents, which in the past had been a useful tool for counterintelligence.

In 1998, DOE moved to include all Top Secret documents under its rules for modified accountability. Sandia National Laboratories elected not to implement that directive, but retained full accountability for all Top Secret data. Sandia is evaluating various implementation modes for restoring document accountability for Secret data as well, even though DOE has not reversed its policy.

As I stated in my testimony, we are implementing an Integrated Safeguards and Security Management System (ISSMS) that will measure and evaluate actual security performance. Thus, we are going beyond mere compliance with the applicable DOE directives for security to a systems approach that constantly measures, evaluates, and improves actual security performance.

Q2: *You also stated in your testimony that you were pleased by the recent passage of a provision in the Defense Authorization Act that will require Q clearances for all employees who work in areas in which classified information is stored or used -- in essence, a return to pre-1994 DOE policy. But this fact will not eliminate your responsibility to control need-to-know in such settings -- indeed, it may make that task more difficult. What are your plans for handling this task?*

Response:

I am pleased that an important objective of the Defense Authorization Act for Fiscal Year 2000 was to strengthen personnel security at all of the national laboratories.

A Q-level clearance in itself does not give a person blanket authorization to access nuclear weapon design information (called "restricted data" or "formerly restricted data") because the "need-to-know" principle remains in effect and must be satisfied before such access is granted. On the other hand, a Q clearance does guarantee that an individual has had a full background investigation performed by the Office of Personnel Management or the Federal Bureau of Investigation that qualifies him or her to view or handle restricted data when it is determined that a need-to-know exists. The background investigation required for a Q clearance is significantly more thorough than that required for an L clearance.

The responsibility for determining an individual's need-to-know remains with the holders of the information or the management of personnel whose jobs require them to have access to restricted data. An effective security education program is necessary to ensure that people who manage restricted data are fully aware of their responsibilities with regard to need-to-know. With the influx of L-cleared people a few years ago, our awareness programs had to address the management of two classes of clearances. With the plan to return to all Q personnel, Sandia can focus its training on how to administer the need-to-know principle for a single class of cleared employees. Full training and information will be given to people who manage restricted data regarding their responsibilities in determining the need-to-know status of persons before they release restricted data to them.

Q3: *You noted in your testimony that the lab has taken action to improve protection of classified weapon parts since the inspection by Mr. Podonsky's team. But why did you permit such parts to be stored in unsecured facilities in the first place, and for how long did that situation exist? Did you believe that leaving classified weapons in unsecured facilities, without alarms and without reasonably timely guard checks, met DOE requirements, or any common sense notion of proper security?*

Response:

In answer to this question, it is important to state unequivocally that Sandia never has and never will allow classified weapon parts to be stored in unsecured facilities. The parts in question were always stored within locked, access-controlled facilities located in limited (secure) areas at the laboratory. A limited area is one protected both by fences and guards in which classified materials are authorized to be handled.

As I stressed in my testimony, security protection is achieved by putting multiple levels of protection into place, so that any shortcoming in one level does not expose the protected material or parts to high risk.

That said, however, Sandia did indeed improve the protection of certain parts as a result of the inspection by Mr. Podonsky's team because some shortcomings that needed to be corrected were discovered during the audit. Those shortcomings were related to patrol frequencies and certain access control features, and they were fixed immediately during the audit. The issue was one of enhancing the level of protection of classified parts that were already protected by several layers of security.

Q4: *You testified that Sandia has increased the frequency of its patrols covering the open storage of classified weapon parts, to address recent inspection findings. What frequency is Sandia conducting now, and do you believe it is adequate to meet DOE requirements?*

Response:

While exact patrol frequencies are classified for obvious reasons, they are based on requirements in DOE Manual 5632.1C-1 and subsequent manuals that govern how frequently an area must be visited to meet certain DOE protection criteria. Sandia did, however, increase the patrol frequency for certain buildings as the result of the safeguards and security inspection. We believe that our new patrolling schedules are adequate to meet both DOE requirements and appropriate levels of protection.

Q5: *According to a June 1999 memo from the Energy Secretary, DOE is drafting a new contract clause that would place the labs' annual performance fee at risk if they fail to achieve a satisfactory rating in an evaluation of their performance under their security plans.*

Would you agree to forfeit your lab's performance fee or senior management bonuses if the lab received marginal or unsatisfactory ratings in any security area? And would you be willing to have independent inspections determine the ratings, as opposed to the DOE field office annual surveys?

Response:

Consistent with my statement, we are willing to consider changing the conditions of our contract in a bilateral and equitable manner. The additional condition at issue—fee and personal compensation “penalties”—are more severe remedies than we currently have and were not part of the original business arrangement when the contract was executed about six years ago. This proposed condition would introduce more risk into the operation of the

laboratory than was contemplated at the outset. There are ways of mitigating this risk, such as clearly specifying the reasonable standards against which our security performance would be measured and providing the additional resources with which lab management could put the necessary control mechanisms in place. Another mechanism would be to provide positive monetary incentives for performance in excess of the agreed standards. Whether DOE were to employ an "independent" assessment or continue to rely on the DOE field operations oversight should matter little; both techniques would have to allow for a well defined set of criteria that would be used to plan and execute a systematic approach to security.

Currently, Sandia Corporation operates under a cost-plus-fixed-fee contract. Sandia and DOE both believed that this form of contract was the most effective arrangement for managing the laboratory to achieve its mission goals without fostering an inordinate focus on financial incentives and penalties. Substantial "incentives" to perform well are anchored in DOE's Laboratory Appraisal system, negotiated and overseen by the DOE field office. More than a survey, the annual appraisal is a rigorous process that results in a grade reflecting the quality of management's performance. We believe this system has served DOE well, and we would want to exercise careful judgment before any drastic changes were contemplated. The insertion of the changed contract term at issue, would effectively require a restructuring of the contract to assure that we minimize the distractions from our national mission, to keep us focused on our important mission goals, and to ensure equity to both parties.

We would urge DOE to carefully consider the long-term impact of substantial new conditional performance penalties on its ability to enlist the nation's foremost technological firms and research universities as contractors for its laboratories. The management fees currently provided (on the order of \$10-20 million per year) are modest in the context of the consolidated earnings of major corporations, and have never been the primary motivation for either corporate or not-for-profit M&O managers. If new contractual penalties increase the business risk of managing a laboratory to an unacceptable degree, the quality of contractors attracted to bid for DOE M&O contracts will most certainly decline.

Q6: *The Committee understands that each of the labs permits foreign nationals from sensitive countries like China, Iran, Pakistan, and Russia to have authorized user status on their unclassified systems -- either on site or via remote dial up, or both. Is that correct with respect to your lab, and if so, what are the actual numbers from each sensitive country?*

Prior to the recent inspection, how did your lab ensure that these Chinese or Russian nationals were not gaining access to information that they do not have any need to know, or are prohibited by law from seeing? Was there anyone monitoring them? Did the lab conduct background checks on these foreign nationals prior to granting them authorization to access the computer systems?

What steps have you taken since the recent inspection to tighten controls on such access, and to implement the new DOE policy on cyber access by foreign nationals?

Response:

Sandia has three levels of network—open, restricted, and classified. The Sandia Open Network includes Sandia's Internet server, which is open to the Internet universe. Protected islands of sensitive information (export controlled or proprietary) are permitted on the Sandia Open Network for collaboration with some corporations and universities. Authorized access to these islands is controlled by DOE-approved security measures. Within these islands, DOE-approved need-to-know restrictions are implemented to further protect this data. Foreign nationals from sensitive countries may be granted access only to those portions of the Sandia Open Network required for approved activities. If access is granted, foreign nationals access the appropriate parts of the Sandia Open Network with a password. No foreign nationals from sensitive countries are currently permitted access to any of the islands which contain sensitive information. The Sandia Open Network permits collaboration with researchers at universities and in industry in areas of unclassified basic research that is of generic interest to the scientific community.

Sandia currently has 13 foreign nationals from sensitive countries with access to its open network. These individuals are from China (7), India (3), Russia (2), and Taiwan (1). Indices checks were performed on these individuals before they were granted accounts on the Sandia Open Network.

The Sandia Restricted Network contains sensitive unclassified information, including official-use-only and proprietary information. There are no foreign nationals from sensitive countries currently on the restricted network. None are allowed on the classified network.

At the time of the recent inspection, two foreign nationals from sensitive countries had been authorized for remote access to the Sandia Restricted Network. We performed indices checks on these individuals before granting them authorization to access the network. Both were permanent resident aliens and therefore treated under the same rules as U.S. citizens with respect to export controlled information. Their access to the Sandia Restricted Network was controlled by means of a SecurID card and password, which provides strong two-factor authentication. Intrusion detection software on the Sandia Restricted Network would have detected suspicious behavior had these individuals attempted to defeat network security features.

As a consequence of the recent inspection, we removed the two foreign nationals from sensitive countries from the Sandia Restricted Network. At this time, no foreign nationals from sensitive countries have access to Sandia's restricted network. We are currently revising our approval procedures to incorporate risk assessments to the approval process for foreign nationals. We will not permit foreign nationals from sensitive countries to have access to Sandia's Restricted Network in the future until the approval process and security plan for such access is revised and approved by DOE.

Q7: *Mr. Podonsky's team found various computer security vulnerabilities at the labs, such as passwords, firewalls, transfers from classified to unclassified systems, among others. Most, if not all, of these issues had been raised in earlier inspection reports dating back to 1993 and 1994. Why did your lab fail to address these computer security vulnerabilities for so long, and why did it take the recent inspection and directives from the Secretary to prompt improvements in this area?*

Response:

With respect to safeguards and security evaluations of Sandia National Laboratories in years prior to 1999, it is not accurate that issues were raised relating to passwords, firewalls, file transfers, and so forth. On the contrary, the 1995 inspection (none were performed in 1993 or 1994) by the DOE Office of Security Evaluations [OS Doc. No. OS-S-95-00245] stated that "sensitive unclassified information is appropriately protected, and security features are adequate to prevent computer system penetration from the Internet"; and, "The classified internal secure network is well defined overall and very well implemented." The next safeguards and security evaluation, occurring in 1997, contained similar expressions of confidence in Sandia's firewall and password systems.

Notwithstanding the generally positive findings of previous inspections, Sandia vigorously addressed any identified deficiencies according to the action plans for each finding. Significant enhancements to the corporate-wide system for issuing passwords were implemented in 1998 to further strengthen our passwords, and a means to identify and disconnect systems with weak passwords was developed in 1999.

The development of our firewall and the three-level network began in 1989 and reached substantial maturity in 1995. The firewall has been continually improved over the years, and we have continually evaluated commercial firewalls to look for opportunities for improvement. Unfortunately, the most popular commercial firewalls were from foreign vendors and constituted an unacceptable potential vulnerability by a foreign government. Therefore, we have resisted the urging to adopt a commercial firewall product until a suitable domestic supplier was found. We have procured a promising domestic firewall and are now testing it. If the tests are successful, we will deploy it.

Mr. Podonsky's team found a number of potential vulnerabilities on the sensitive unclassified network behind the firewall. We have aggressively addressed these issues since the audit. These potential vulnerabilities increased the importance of the firewall in our layered approach to cybersecurity. Mr. Podonsky's team found our firewall to be generally robust but identified one potential vulnerability that needed further investigation. Further analysis of that possible vulnerability indicated that the result was a false positive (which is to be expected occasionally in the diagnosis of such a complex system). We have communicated these results to DOE and they are analyzing our report. The robustness of our firewall has been subsequently corroborated by the DOE Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory. Consequently, we continue to have confidence in the Sandia firewall for the immediate future while we take the appropriate time to properly qualify a replacement firewall. We shared this information with Mr. Podonsky's team during their follow-up visit to Sandia during the week of December 6 through 10, 1999.

Q8: *You testified that, although no Sandia employees have been polygraphed to date under the DOE's recently proposed polygraph program, several hundred Sandia employees have been polygraphed over the years under various existing programs. Can you provide more specific information about the number of employees, by year, that have been polygraphed, and identify the specific programs under which they were polygraphed? If the names of the programs are classified, please simply indicate whether the programs*

are run under your contract with DOE or whether they are programs run under "work for others" contracts, such as with the Defense Department.

Response:

My testimony was that just under 200 people have been polygraphed at Sandia.

Sandia National Laboratories does not conduct polygraph examinations and does not keep formal records of polygraph exams performed on Sandia employees by sponsoring agencies. Rather, such records are maintained by the agencies in the defense and intelligence communities that require and perform the tests. For a precise accounting, including the identity of the classified programs for which the polygraphs exams were performed, the committee may wish to request this information from the agencies that required the polygraph examinations. If desired, we will furnish the names of those agencies to the committee under separate cover protected as confidential national security information.

Our count of the numbers of polygraph examinations performed on Sandia National Laboratories employees from 1979 through 1999 is shown in the table below. This table is not based on official agency records (to which we do not have access), but is our own informal count.

Polygraph exams are considered current for five years. Consequently, some employees have been polygraphed more than once. During the period covered by the table, ten employees were polygraphed twice. Thus, the number of persons represented in the table is 166. The table does not include polygraph examinations on employees who have retired, and is therefore somewhat understated.

With one exception, all these polygraph examinations were performed for and by various agencies in the federal defense or intelligence communities in classified programs under work-for-others agreements. A single polygraph examination by DOE occurred in 1989 in association with a program related to NSDD-281, signed by President Reagan.

**Sandia National Laboratories
 Approximate Number of Polygraph Exams, 1979-1999**

Year	1999	1998	1997	1996	1995	1994	1993
No. of polygraph exams	18	28	26	0	3	71	2

Year	1992	1991	1990	1989	1988	1987	1986
No. of polygraph exams	1	4	5	2	0	0	1

Year	1985	1984	1983	1982	1981	1980	1979
No. of polygraph exams	2	6	0	1	1	0	5

Approximate no. of polygraph exams, 1979-1999 = 176

Q9: You also testified that your corrective actions dealing with the issue of classified matter repositories has been/is being delayed due to disagreements between two offices within DOE as to the proper type of repository needed. Can you explain this matter in more detail, specifically including information relating to the DOE offices involved, the nature of the disagreement, and how that has impacted your corrective actions?

Response:

DOE orders require that classified documents and materials be stored in containers approved by the General Services Administration (GSA). In those cases where classified material, because of size, weight, or construction, cannot be stored in GSA-approved containers, a vulnerability analysis of the non-standard storage alternative must be conducted. At the time of the inspection by Mr. Podonsky's team, we were using storage containers for documents that had been approved under a variance granted by the local DOE field office. The inspection team from DOE headquarters disagreed with the use of those containers for storage of classified documents. They were also concerned with non-standard storage of classified matter. To address these concerns, the parties have agreed to a multi-faceted approach which will include vulnerability analyses of facilities, reactivation of vaults, modifications of rooms into vault-type-rooms (VTRs), and ordering GSA-approved containers where feasible. While these actions are being completed, affected classified matter is being placed in interim storage facilities that are either vaults or will be manned twenty-four hours a day.

Q10: During the hearing, Congressman Stupak requested that you provide for the record a list of those security and safety improvements that Sandia has implemented over the years on its own -- that is, without being directed or persuaded to do so by any element of DOE (including the field office, headquarters, and Mr. Podonsky's office). Please provide a list of such improvements, limited to significant measures undertaken during the last five calendar years.

Response:

The following list illustrates some of the many improvements and innovations in security and safety implemented on the initiative of Sandia National Laboratories without directive from DOE elements or the Defense Nuclear Facilities Safety Board:

Computer Security

- Sandia pioneered the **three-level network security architecture** that has been accepted as the standard configuration for the nuclear weapons complex in 1999. This architecture includes an unclassified, non-sensitive external network open to the Internet and our university and industrial collaborators; an unclassified internal restricted network accessible only by personnel with authorized access; and an internal classified network secured by personnel clearances, strong authentication systems, encrypted communications, need-to-know groupings, and hardware/software isolation from unclassified systems.

- At the creation of the Sandia Restricted Network (which contains sensitive unclassified information), Sandia developed a restrictive **firewall** to protect this network from the Internet. The capabilities of the firewall have been enhanced through the years to provide greater utility for Sandia's scientists and engineers while presenting a significant barrier to unauthorized access from the Internet.
- A proxy server for the worldwide web was implemented at Sandia National Laboratories in 1995 with a set of filters developed by Sandia that **strengthened the firewall** by allowing users to access web pages on the Internet while preventing the automatic execution of dangerous file types. Filters installed at the Internet point of connection prevent other sites from masquerading as Sandia addresses and inhibit other common attacks.
- In 1995, Sandia implemented a **network intrusion detection system** using the "NID" software developed at Lawrence Livermore National Laboratory. In 1999, Sandia is in the process of replacing NID with an improved commercial package, "RealSecure" from Internet Security Systems.
- Sandia has recently **developed another firewall** called "FTP Guard," which runs on an operating system approved by the National Security Agency, to protect against file transfers out of the classified network. FTP Guard is a "diode" filter that, when implemented, will permit users on the Sandia Internal Secure Network to download unclassified files from an unclassified network while preventing file transfers in the opposite direction. FTP Guard has passed multiple independent technical reviews and is the first system of its kind to be accredited by DOE. We expect FTP Guard to be implemented on our production network at an appropriate time in the future.
- Sandia, in cooperation with Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and DOE nuclear weapons production agencies, developed a **secure, high-speed, intersite network** linking the classified networks at each of the nuclear weapon laboratories and the production plants. This wide-area network, called "DOE SecureNet" was conceived and designed by the laboratories.
- Sandia adopted the **Kerberos network authentication protocol** developed at the Massachusetts Institute of Technology. Kerberos provides strong authentication for client/server applications by using secret-key cryptography. Sandia developed a web-based password management system to support our use of Kerberos by assigning randomly generated alphanumeric, mixed-case sequences as passwords. We also developed software to implement Kerberos authentication in the Netscape web browser, providing secure web access to sensitive unclassified information on the Sandia Restricted Network. The draft DOE order on password protection essentially institutionalizes this security feature pioneered by Sandia. Sandia now uses a secure, heterogeneous Distributed Computing Environment from The Open Group, a consortium of vendors, which incorporates the Kerberos authentication system.
- Sandia implemented an **Entrust public key infrastructure** on its unclassified restricted network in 1997, enabling secure exchange of sensitive unclassified documents via encryption and digital signature within the laboratory and with other DOE sites.

- In 1998, Sandia began a **network scanning process** (using ISS/CyberCop) almost a year before the Tri-Lab InfoSec Plan recommended it.
- In 1999, Sandia added **SecurID authentication** to ISDN dial-up access to its unclassified networks. A SecurID card provides strong two-factor authentication.
- Sandia wrote **security configuration guidelines for classified and unclassified desktop systems** in 1999. Desktop security models for PCs (Windows), UNIX, and Macintosh systems are providing uniform definition and automated monitoring to reduce vulnerabilities.

Physical Security

- Between 1996 and 1999, Sandia National Laboratories, New Mexico, installed **automated security gates** at 24 portals to control access by pedestrians and vehicles into the laboratory's technical area. This system improved security by using magnetic-strip badge readers rather than visual inspection by security guards, which can be unreliable, especially during peak traffic times.
- In 1998, Sandia spent \$500,000 on **equipment for technical security countermeasures**, which was not yet required by DOE but which we felt would increase the reliability of the system. It is our understanding that DOE plans to require the new equipment at DOE sites in the next few years.
- Three years ago, Sandia National Laboratories, California, **replaced its alarm system** using laboratory funding rather than line item funding. The California site has installed extensive access control features, allowing owners of limited areas to grant access to rooms and areas based on need to know. We intend to install a similar system at New Mexico as funding permits.

Personnel Security

- In 1997, Sandia established an **Infraction Review Committee** to process and evaluate security infractions. This committee is composed of the manager of the security incident management program, the line manager of the person responsible for the potential infraction, and the manager of the safeguards and security topical area involved in the incident. Incidents from special access programs and sensitive compartmented information facilities are also reviewed by this committee.
- In 1999 Sandia implemented an **electronic Foreign National Request (FNR) System**. Web-based and user-friendly, the system uses a workflow system and parallels the concurrence process to improve data quality, facilitate approvals, eliminate data re-entry, and provide users with on-line access to unclassified data regarding the status of visit requests. Other laboratories in DOE and DoD have asked Sandia to share these programs with them.

Security of Nuclear Materials

- In 1995, Sandia completed a site-wide plan for **disposing excess nuclear material**. Since then, more than 20 metric tons of accountable nuclear material has been shipped from Sandia, either for recycling or disposal as waste. The benefits of this reduction in inventory include reduced vulnerability, lower protective force

costs, and consolidation of material into facilities specially designed to protect nuclear material.

- In 1997, we implemented the **Sandia National Laboratories Local Area Network Materials Accountability System (SNL-LANMAS)** to maintain the laboratory's book inventory of nuclear materials. SNL-LANMAS tracks nuclear materials in storage and transport and calculates the radioactivity and decay rates.

Environment, Safety, and Health (ES&H)

- Sandia National Laboratories was one of the first Department of Energy facilities to institute an **Integrated Safety Management System**, and did so before it was mandated.
- Sandia developed **automated risk management tools** that assist in the identification, evaluation, and control of hazards; generation of safety-basis documentation; maintenance of safety-critical building systems; and tracking of safety and security issues. These tools include the following modules:
 - **Primary Hazard Screen** module is a series of successive question sets that link work hazards to program requirements, recommended work controls, and training guidance in the ES&H Manual covering all work activities.
 - **Hazard Analysis** module contains scenario templates and more detailed analysis question sets related to low-hazard facilities and operations.
 - **NEPA/ADM** module is a checklist for determining actions and project documentation required for compliance with the National Environmental Policy Act.
 - **Maximo** database automatically schedules maintenance of safety-critical building structures, systems, and components in terms of priority and frequency.
 - **Sandia Issues Management System** database supports tracking of safety and security issues and corrective actions, and roll-up for reporting to executive management.
- Sandia developed a **Chemical Information System**, which is a set of networked chemical management databases supported by a field team of inventory specialists. We connected the local fire station on Kirtland Air Force Base to this system so that firefighters can determine what chemicals may reside in Sandia buildings when they respond to emergencies. The Chemical Information System includes the following elements:
 - **Chemical tracking database** allows tracking and inventorying of bar-coded chemical containers from purchase to disposal.
 - **Material safety library** has more than 60,000 Material Safety Data Sheets available on-line for managers and personnel to use in understanding and controlling chemical reactions and exposures.
 - **Chemical exchange service** supports the redistribution of surplus chemicals for reduction of existing inventories and new chemical purchases.

- In 1997, Sandia established a **database for construction safety inspections**. This item was cited as an "area of excellence" in the DOE laboratory appraisal report for that year. In addition, we implemented a safety incentive program which rewards subcontractors for safe performance of job duties.

Education and Training for Security and Safety

- Sandia created a suite of **interactive training courses on the Sandia internal web site** for security and ES&H. This computerized training system provides flexible delivery options and automated record-keeping of training compliance. User-friendly modules with test questions include initial and refresher courses on general security, computer security, classification and document control, ES&H awareness, and general employee radiological training. The Training and Educational Development System database is a course management software application that lets management assign, track, and enforce course completions for all personnel.

Programmatic Security Research and Development

In addition to the security actions listed above, security technologies pioneered by Sandia include a wide range of security concepts, systems, and components proposed and developed in the national interest.

- In 1999, Sandia National Laboratories developed the **world's fastest encryptor chip** called the "SNL Data Encryption Standard (DES) Application Specific Integrated Circuit (ASIC)." It is the fastest known implementation of the DES algorithm, a mathematical transformation commonly used to protect data by cryptographic means. The device encrypts data at more than 6.7 billion bits per second, 10 times faster than any other known encryptor.
- **Activated denial concepts** are used to convert benign operational working environments into unfriendly ones upon detection of an adversary attack. Activated denial technologies developed by Sandia and used throughout the DOE include smoke dispersal systems, aqueous foams, and sticky and rigid foams.
- **Explosives detection** of vapors or particulates is an area where Sandia now holds multiple patents. We are providing licenses to industry to commercialize walk-through detectors of molecules of explosive compounds, suitable for use in airports.
- **Architectural surety** is a concept developed at Sandia as a response to the Oklahoma City bombing in April 1995. It applies multi-level surety principles developed in the nuclear weapons program to the design of civil structures. These principles can be applied to many civilian situations that involves high consequences (e.g., air travel, storage of spent nuclear fuel, critical infrastructures). A graduate course in architectural surety has been taught in cooperation with the University of New Mexico's Civil Engineering Department, and other universities are developing partnerships with Sandia to offer courses in architectural surety.
- Sandia National Laboratories develops **technologies for safely disabling terrorist bombs**. Every year, in cooperation with the FBI, Sandia conducts advanced training for bomb squads of police departments, emphasizing the science,

technology, and practice of bomb disablement. We entered this work on our own initiative because our expertise in chemical explosives and detonation systems for nuclear weapons could be applied to this important public safety issue.

- In 1996, Sandia National Laboratories installed a suite of security systems at a high school to demonstrate the application of technologies appropriate for **school security and safety**. The school reported a 90 percent decrease in vandalism and theft and a 75 percent decline in fights on campus. Since then, Sandia has advised administrators at more than 100 schools nationwide. In cooperation with the National Institute of Justice, we have made available—as a public service—a manual entitled, “The Appropriate and Effective use of Security Technologies in U.S. Schools.” This manual is downloadable from the DOE and Department of Justice web sites.

DOCUMENT NO: OS 5-44-00452
DOCUMENT CONSISTS OF 25 PAGES
CY NO. 1 OF 2 CYS. SERIES A

QUESTIONS FROM THE HOUSE COMMITTEE ON COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS (U)
SUBMITTED TO MR. GLENN PODCANSKY, DOE 11/2/99

- Q1.a. (U) You mentioned in your testimony that, at all three weapon labs, the storage of classified weapon parts was a problem. Can you be more specific about the types of weapons parts at issue – for example, are they minor, unassembled components, or are they complete missiles or warheads?
- A1.a. (U) The weapons parts involved included an extremely wide spectrum of types, quantities, and ages. Some storage locations housed individual weapons components, others housed various weapons assemblies and sub-assemblies, and still others housed full weapon mock-ups or “trainers” containing all internal components except the special nuclear material and the high explosive. Some parts, assemblies, or mock-ups were considered obsolete, and others were current-inventory items.
- Q1.b. (U) In what types of structures were these missiles and other parts stored in, and what type of security systems, if any, existed in these structures?

[REDACTED]

[REDACTED]

- Q3.a. (U) In Livermore's corrective action plan, the lab notes that it will have 2-hour guard checks for these open storage locations, while Sandia simply notes that it has increased its frequency of guard checks. Are you comfortable that these time frames would allow for timely detection and retrieval of any stolen parts? And what if someone didn't want to steal a part, but just photograph it?

[REDACTED]

- Q3.b. (U) Do you believe that the corrective actions to date implemented by Los Alamos, Sandia, and Livermore with respect to protection of classified parts comports with DOE security requirements?

[REDACTED]

[REDACTED]

[REDACTED]

- Q6. (U) Similarly, at Sandia, you found problems with "access controls in areas where classified matter is used and stored." Can you provide some examples

[REDACTED]

- Q7.a. (U) At Livermore and Sandia, you also found problems with storage of classified documents and other media in non-approved containers. Both sites say that corrective actions to address this finding will take at least a year to complete, maybe longer, and, in the meantime, they will conduct random guard checks of these storage containers. Do you believe these actions are adequate to ensure the security of these important materials, and to bring the labs in compliance with DOE requirements?

[REDACTED]

[REDACTED]

Q7.b. (U) Ms. Stone of your Office accompanied Committee staff on a visit to Livermore several weeks ago, and during this visit, learned more information about the actual implementation of random guard checks and the lab's efforts to consolidate materials into approved safes. Based on that more recent assessment, are you able to discern any attempt by Livermore to prioritize its assets to ensure that guard checks of the most sensitive materials occur more frequently, or that the most sensitive materials stored in unapproved containers are being transferred according to any priority?

A7.b. (U) Livermore has a corrective action plan in place and has made some progress in upgrading containers and moving the most sensitive classified matter to more secure storage locations. The degree to which these actions resulted in increasing the security of the most sensitive assets will be reviewed during the scheduled follow up visit to Livermore.

Q7.c. (U) Did Ms. Stone find examples where there was no apparent record of any guard check so far, even though they were supposed to begin back in July?

[REDACTED]

Q8. (U) Another problem you identified at Sandia had to do with controls of foreign visitors and assignees, including some from sensitive countries. Can you explain what you found in this area, and whether there is any reason to believe that these problems may have resulted in the compromise of classified information? Would the labs be in a position to know whether any such compromise may have occurred?

[REDACTED]

[REDACTED]

- Q9.b. (U) Based on these tests and vulnerability scans, is it your belief that your cyber team would have had an unlimited ability to move freely throughout the labs' unclassified systems once penetration was accomplished? Did, in fact, your team do so?
- A9.b. (U) It should first be noted that the Los Alamos firewall was deemed to be adequately designed and configured at the time of the most recent inspection. Additionally, Los Alamos had an effective policy for identifying and removing unauthorized modems.

[REDACTED]

[REDACTED]

Q10.a. (U) You testified about several computer security issues, such as passwords, firewalls, transfers from classified systems, among others. Are these issues new, or were they raised by your Office prior to these recent inspections?

[REDACTED]

[REDACTED]

Q10.b. (U) If so, what was the response of the labs and the DOE hierarchy to your findings on computer insecurity? Did they tell you they would rather accept the risk of these vulnerabilities than fix the problems?

A10.b. (U) Livermore and Sandia committed to fix the vulnerabilities identified during the inspections and developed corrective action plans to do so. Independent Oversight (then known as the Office of Security Evaluations) was not included in the review process for site corrective action plans during that time. These corrective action plans were reviewed during subsequent inspections and Independent Oversight found many cases where the labs did not effectively identify the root causes of the problems and repeat findings were issued.

[REDACTED]

Q11. (U) Given the years of unresolved vulnerabilities on these computer systems, is there any way for you or the Department to gauge the extent of possible compromises to

national security from the computer security problems your Office has identified in reports dating back to 1994?

- A11. (U) It would be difficult for Independent Oversight to gauge the extent of possible compromises. Independent Oversight has not traditionally been in the reporting chain for computer security incidents. In fact, DOE sites are encouraged to report all incidents to the Department's Computer Incident Advisory Capability (CIAC), who reports to the DOE Chief Information Officer (CIO). It should be noted that the CIO has recently begun providing periodic CIAC summaries to Independent Oversight. However, CIAC would only know about "reported" incidents. Given the history of computer security vulnerabilities identified by Independent Oversight, it is likely that many unsuccessful and successful penetration attempts of unclassified networks containing sensitive information have gone unnoticed.

[REDACTED]

[REDACTED]

Q12.b. (U) Once these foreign nationals were given authorized status, did they have links to other sites within or outside of DOE?

[REDACTED]

Q12.c. (U) Lawrence Livermore notes that it now has intrusion detection software in place at the border of its open network to monitor the situation with remote access by foreign nationals. But will intrusion detection at the open border really inform the labs what these foreign nationals are doing once they get inside? If they are authorized users, will intrusion detection techniques enable the labs to restrict access to sensitive information by sensitive country foreign nationals?

A12.c. (U) Intrusion detection will only inform the labs if foreign nationals (or any other user) attempt to use known techniques to access other systems on the network. The only way to know what the foreign nationals are doing is to specifically target their accounts and monitor all access to and from their computer. Intrusion detection can provide significant deterrence, but will not restrict authorized users from accessing sensitive

information. Intrusion detection merely informs system administrators of malicious activities after they are detected.

Q12.d. (U) How would DOE or the labs know if someone dialing in from a remote site, like a foreign country, really was the authorized individual?

A12.d. (U) There is no way to be absolutely sure of the individual at the other end of a connection. Even if "smartcards" are used to generate disposable passwords, DOE and the labs cannot be sure that the authorized user did not loan or give away the smartcard and personal identification number needed to make it work.

Q13. (U) If a Russian or Chinese national wanted to gain physical access to one of these labs, DOE would require that a background check be done to ensure that the individual does not have ties to intelligence agencies, and also would require that a security plan be established for that individual in order to control his or her access to classified information. But were the labs doing background checks (that you could verify) and creating security plans before giving remote computer access to these same individuals? If not, why not, and what type of risk were the labs taking?

A13. (U) At the time of the last inspection, Livermore's practice was to permit foreign nationals to access the network based solely on the approval of the sponsor and the computer security organization. Foreign national access was then allowed subject to procedures contained in the Livermore computer security plan for foreign nationals.

(U) Sandia and Los Alamos required that all foreign nationals be processed through the Foreign Visits and Assignments Office, even though there was no policy specifically requiring this. Since the computer access was to unclassified systems, there was no requirement under foreign visits and assignments requirements for a security plan and none was prepared.

(U) Independent Oversight conducted random checks to verify that these local practices were implemented as specified in local procedures.

(U) On November 1, 1999, DOE issued DOE Notice 205.2 that sets new requirements for allowing foreign nationals access to cyber systems.

Q14.a. (U) During the hearing, Ms. Stone of your Office testified regarding the matter involving Livermore's reliance on local law enforcement to handle certain aspects of its security, but deferred certain questions for the record. Please provide the following information on this matter:

(U) When did Livermore make the change to rely in part on local law enforcement, and was your Office involved in any contemporaneous discussions or analyses of this matter?

[REDACTED]

Q14.b. (U) What analyses did DOE or Livermore perform at the time to justify this switch, and was it adequate in your opinion?

A14.b. (U) The Livermore analysis and performance testing that determined that the change was appropriate was conducted using the Analytical System Software for Evaluating Safeguards and Security (ASSESS) computer model and expert judgement. This was the best technique generally available to the Department at the time. The model treatment of the tactical engagement of the adversaries by the protective force is unsuitable for most tactical considerations, but was supplemented by the judgement of a number of laboratory and DOE security experts. In addition, the results of performance tests conducted by Livermore and by Independent Oversight supported the general conclusions reached in the computer analysis. Based on the attractiveness of targets at the laboratory at that time and on the state of computer modeling within the DOE at that time, the modeling was adequate.

Q14.c. (U) When did your Office first raise concerns about this matter, and what did your own analyses reveal about the effectiveness of Livermore's reliance on local law enforcement? Specifically, what were the expected and actual time lines for response, and were either adequate in your opinion?

[REDACTED]

[REDACTED]

Q14.d. (U) Do you believe that any change in the overall or Design Basis Threat during the relevant time period justified the change to reliance on local law enforcement by Livermore?

[REDACTED]

Q15.a. (U) Back in March, the labs and Secretary Richardson announced a 9-point computer security plan, most of which was supposed to be in place within 30 days, or by May 1, 1999. One action item was to eliminate the possibility of data espionage within a single office, by making the classified and unclassified computer systems physically incompatible.

(U) Where are the labs with respect to this action item, and is it now impossible to transfer data between these two systems?

[REDACTED]

Q15.b. (U) What about the ability of someone to simply download classified information to removable media and take it out of the lab? Has that scenario been closed off yet?

[REDACTED]

Q16.a. (U) Another Tri-lab action item required the labs to enhance their need-to-know controls on their classified computer systems, but it seems from your reports that very little, if anything, has been done in this regard. Is that true?

[REDACTED]

Q16.b. (U) Is it still the case that many divisions within these labs continue to utilize common need-to-know standards for both digital and paper classified records, and if so, does that comport with DOE requirements and good security practices? Why should someone working on one type of warhead be able to gain unfettered access to information about others?

A16.b. (U) According to DOE policy for accreditation of classified computer systems, need-to-know is determined by the data owner. At the labs, the data owner is typically at the division director level. Technically, these data owners are conforming with DOE policy when they determine that an entire division shares a common need-to-know. However, good business and security practices suggest that data be shared only when actually necessary. While we agree that there may be individual cases where a person designing a certain warhead may need access to specific information from a different warhead design,

we believe that this access should be strictly controlled and revoked when no longer needed.

Q17. (U) In addition to the 9-point plan, the Secretary announced in May an additional six computer security enhancements that the labs would implement in the; quote, "near term." These included conducting random audits of individual computers, imposing stringent printing and logging controls, preventing coded or encrypted messages from leaving the labs via e-mail, and regulating downloads from classified computers.

(U) The Committee understands from your report on Sandia that the lab has not done anything yet in these areas because it is awaiting clearer guidance from DOE. Is that correct, and what, if anything, have the other labs done so far to meet these "near term" goals?

A17. (U) It is correct that Sandia had not done anything to address the six further enhancements at the time of the most recent inspection. According to Albuquerque Operations Office computer security officials, the decision to take no action toward implementation of the six further enhancements was made by the Operations Office because the six further enhancements had not been disseminated through established channels and therefore were not considered official requirements. The same was true for Los Alamos, since they are also under the purview of the Albuquerque Operations Office. However, Los Alamos had taken some steps toward addressing some of the six further enhancements as long as they were not resource intensive. The six further enhancements were released during the latter part of the Livermore inspection. As a result, Independent Oversight has no direct knowledge of the Livermore status. All three labs have indicated in corrective action plans that the six further enhancements will be implemented. Independent Oversight will evaluate the status during the December 1999 follow-up reviews.

Q18. (U) In your opinion, are DOE policies adequate to ensure uniform, minimum requirements for the training of the protective force that guards special nuclear materials and classified weapons across the DOE complex?

A18. (U) Our inspections have not identified systematic weaknesses in protective force performance that are related to training policy and standards. However, there is an opportunity to improve in the area of large-scale performance tests.

(U) DOE policy requires at least one large scale exercise per year to show that the planning assumptions in site security plans are valid. Since these large scale exercises are very expensive, some sites only conduct the one required test and that one is focused on validation of assumptions rather than training. By necessity, such tests are usually conducted at night or on a weekend when facilities are not in use. At some sites, this tends to focus the testing on specific shifts, thereby limiting the number of protective force members who are likely to participate. In any case, if only one test is conducted, the majority of the protective force will not have an annual exposure to a large scale tactical exercise. Other DOE sites conduct additional tests, since they have several facilities that require annual testing. However, these tests remain focused on validation rather than training and still expose only a portion of the protective force to a realistic tactical environment.

(U) Our inspections indicate that protective forces with wider and more frequent exposure to realistic tactical environments tend to perform better in simulated tactical situations. If the very significant operational and resource issues associated with large

scale tactical exercises could be effectively addressed, the readiness of the DOE protective forces would be improved.

Q19.a. (U) Is it true that DOE assumes in its security planning that personnel in a human reliability program (HRP) will not violate security orders to assist adversaries in theft or sabotage scenarios? If so, do you believe that to be a valid assumption – for example, have there been situations in which HRP personnel have engaged in such activities?

A19.a. (U) DOE guidance recognizes that an employee or another individual with authorized access to key facilities presents one of the most difficult security challenges. The DOE has a number of elements within its safeguards and security program that are designed to reduce the likelihood that an individual having authorized access to a key facility will be able to plan and execute an unauthorized act without prior detection and/or that the consequences of such an act are minimal. However, these programs are not considered to provide absolute assurance. Therefore, DOE vulnerability analyses consider the possible actions of such individuals if they were able to plan and execute some act without timely detection and assessment. In most cases, analyses indicate that some individuals remain capable of committing acts with significant consequences despite effective implementation of these programs. In such cases, DOE requires that the site take all reasonable steps to reduce the likelihood and consequences of such an act. If, after these steps, an unacceptable level of risk remains, the DOE requires that the individuals involved be enrolled in an HRP. ~~For vulnerability analysis purposes only~~, such an individual is then considered willing to only provide information to an adversary group, rather than take a more active part in any unauthorized act.

(U) DOE policy does not explicitly allow sites to assume that HRP individuals will not commit an unauthorized act. An HRP is invoked to reduce the adjectival (low, moderate, high) that a manager must formally accept. The risk the manager accepts includes the risk that the enrollment of selected individuals in an HRP will not prevent or deter them from committing a significant unauthorized act.

(U) While OA is unaware of any actual situations in which an individual enrolled in a DOE HRP has been proven to have committed an unauthorized act in support of an SNM theft, radiological sabotage, or espionage, the experience of other agencies is that similar HRP programs are not always successful. It is possible that the results of some current investigations will reveal similar situations within DOE.

Q19.b. (U) How does that assumption affect our current security posture?

[REDACTED]

(U) DOE has devised a revised review and validation process that is being formalized. This process will provide greater assurance that these and similar issues with the review process will be effectively addressed.

Q20. (U) Are there any non-computer areas where DOE policy is currently inadequate in your opinion to give proper guidance to the sites on security matters?

A20. (U) The following policy issues are extracted from 1999 Independent Oversight reports.

- (U) Policy regarding the requirements for remote access to unclassified DOE computer systems by foreign nationals from sensitive countries has recently been addressed by DOE Notice 205.2. Remote access from non-sensitive countries remains to be addressed.

- (U) DOE policy should be revised to include unclassified computer security as a required topic on security surveys.

- (U) DOE programmatic direction and support for nuclear materials disposition between Environmental Management (EM) and DP does not provide the field with adequate support for their nuclear material management efforts.

- (U) The DOE Office of Security and Emergency operations, in coordination with affected program offices, needs to issue policy on intra-site waste transfer reconciliation. In addition DOE needs to determine if the DOE/NRC Form 741 will be the official accounting records system for WIPP.

- (U) Current policy guidance in DOE M 5632. 1 C- I for calculation of False Alarm Rates and Nuisance Alarm Rates is ambiguous.

(U) In addition, Independent Oversight has provided comments on revised policy in the areas of:

- (U) Combining the Personnel Security Assurance Program and the Personnel Assurance Program; and
- (U) The need for further specificity in the requirements for protection of especially sensitive classified nuclear weapons parts.

Q21. (U) Prior to recent reforms, was anyone at DOE tracking your Office's findings to ensure corrective actions, and was your office involved in validating the closure of such findings? How have things been changed in this regard?

A21. (U) Prior to the recent reforms, Independent Oversight safeguards and security findings were tracked to completion by the cognizant Operations Office and the Office of Safeguards and Security. Independent Oversight was not included in the determination of appropriate corrective actions or the validation of measures taken to close findings. However, Independent Oversight did, as a matter of routine during succeeding inspections, investigate each finding closed since the last Independent Oversight inspection of that site to determine whether the corrective actions taken were effective. The effective closure of Independent Oversight findings, as well as local self assessment issues and security survey findings, has also traditionally been a portion of the analysis

and rating of effective safeguards and security management under the Protection Program Management topic.

(U) If any finding was found to be “closed” by ineffective corrective actions, a repeat finding was issued in the associated technical topical area. If it was found that there was any systematic trend toward ineffective closure of findings, this was reflected in the Protection Program Management topical area.

(U) The Office of Independent Oversight and Performance Assurance continues to include the effective closure of findings as an important element in the review of the Protection Program Management topic. Under the reformed procedure, Independent Oversight is intimately involved in the evaluation of the corrective action plan that describes the actions to be taken to close each Independent Oversight finding. In addition, Independent Oversight has its own tracking and trending system and now conducts follow up visits in between inspections to determine the effectiveness and timeliness of actions taken under approved corrective action plans. Perhaps the most significant change is that Independent Oversight now has a direct reporting path to the Secretary that will enable the Office to bring any issues related to corrective actions directly to senior management attention.



Department of Energy

Washington, DC 20585
June 16, 2000

The Honorable Fred Upton
Chairman
Subcommittee on Oversight and Investigations
Committee on Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On October 26, 1999, Glenn S. Podonsky, Director, Office of Independent Oversight and Performance Assurance; Gil Weigand, Deputy Assistant Secretary for Research, Development and Simulation, Office of Defense Programs; Edward J. Curran, Director, Office of Counterintelligence, and Eugene E. Habiger, General, USAF (Retired), Director, Office of Security and Emergency Operations, testified regarding the State of Security at the Department of Energy's Los Alamos National Laboratory (New Mexico), Sandia National Laboratories (New Mexico), and the Lawrence Livermore National Laboratory (California). On April 5, 2000, we submitted a partial response to the questions for the record.

Enclosed are the answers to questions submitted by Members of the Subcommittee to Edward J. Curran. This will complete the hearing record.

If we can be of further assistance, please have your staff contact our Congressional Hearing Coordinator, Barbara Barnes at (202) 586-6341.

Sincerely,

A handwritten signature in black ink, appearing to read "Tom C. Angel".

Tom C. Angel
Assistant Secretary
Congressional and Intergovernmental
Affairs

Enclosure



**Office of Counterintelligence Response to
Questions for the Record
Hearing of the Subcommittee on Oversight and Investigations
October 26, 1999**

Q1. In your testimony you said, "On November 13, 1998, Secretary of Energy Richardson approved virtually all of the 46 recommendations identified in the 90-Day study..."

What recommendations were not approved by Secretary Richardson?

Why were those recommendations made by you, and why were they not approved by Secretary Richardson?

What consequences are there, in your opinion, to the failure to implement those recommendations?

In your opinion, are those recommendations still necessary? If not, what has impacted the necessity of those recommendations?

A1. The Secretary of Energy's Counterintelligence Action Plan was issued on November 13, 1998, and was written in response to the 90 Day Study completed by my Office in July 1998. The Secretary's Action Plan modified two of the recommendations contained in the 90 Day Study by exempting six facilities from certain foreign visit tracking requirements, and from a requirement that they develop a list of unclassified sensitive technologies at their sites.

The Secretary decided that those Department of Energy (DOE) facilities that did no classified work would be exempt from both increased tracking of foreign visitors, including the strict indices check requirement imposed on facilities that did classified work, and from drafting a list of the sensitive unclassified technologies at their sites. As a result, these facilities¹ are exempt

¹ The Action Plan contained exemptions for six facilities: Ames Laboratory, Fermi National Accelerator Laboratory, National Renewable Energy Laboratory, Princeton Plasma Physics Laboratory, Stanford Linear Accelerator Center, and Thomas Jefferson National Accelerator Facility. A seventh, Lawrence Berkeley National Laboratory, was later added to the list.

from DOE Notice 142.1, *Unclassified Foreign Visits and Assignments*, except for those employees who hold security clearances, and therefore conduct indices checks for only those visitors hosted by employees with clearances. The DOE Office of Counterintelligence (OCI) believes that foreign intelligence services target unclassified as well as classified sites, and unclassified as well as cleared individuals, and thus did not endorse the Secretary's decision. However, OCI maintains CI oversight authority for the entire DOE complex, including these sites.

Q2. As the head of the Office of Counterintelligence, the Committee would like to get your assessment of the threat posed by permitting remote computer access by sensitive country foreign nationals to the labs' computer systems. Do you believe that there is cause for concern about espionage, and if so, what do the labs need to do to properly control such access?

Does the recently-issued DOE policy directive on this matter eliminate your concerns about this practice?

Under your counterintelligence (CI) implementation plan, there are several recommendations that appear related to this issue – one recommends the implementation of intrusion detection programs, while another recommends monitoring and auditing of high risk personnel, while yet another deals with auditing of foreign nationals with remote access to Super Computers. It appears from your status report that little, if anything, has been done in these areas. Can you describe where DOE and the labs are with respect to these three recommendations?

A2. There is cause for concern about espionage in the case where foreign nationals are permitted remote access to DOE computer systems. Due to the current state of security in commercial computer systems (i.e., low levels of security), persons with legitimate access to a computer system often can easily expand their authorization to access information and other systems normally denied to them. Specific counterintelligence concerns include the following:

- DOE systems are significantly interconnected. Providing access to a system at one DOE

site also provides potential access to all DOE sites.

- DOE defense laboratories' computer networks are deployed in a three tiered structure to provide "defense in depth" to each sites' most sensitive information. The most open, the "green" network, contains no sensitive information and provides direct access to the Internet. The "yellow" network does contain sensitive, unclassified information and is protected from the green network by commercial and DOE developed security devices. Classified information exists only in the "red" network. The red network is connected to the yellow network through high assurance security devices. Information may flow from the yellow to the red network through NSA approved unidirectional data movers. These devices do not allow information to flow in the opposite direction. Red networks are interconnected between laboratories using NSA provided cryptographic devices. While the tiered "defense in depth" model is valid from a risk management approach, CI has concerns that the yellow networks are still vulnerable to moderately sophisticated attacks and the red networks may be vulnerable to extremely sophisticated attacks. The data contained within the red network is extremely valuable and must be considered a significant enticement for foreign adversary to attempt to find and exploit a weakness.
- Remote access provides the opportunity for the legitimate user to share their access permissions with other, non-authorized personnel. Additionally, the existence of remote access and remote authentication also provide the avenue for a foreign adversary to forge or hijack a legitimate user's authentication without the cooperation of the legitimate user.
- Due to the remote nature of the access, there is little chance of the intruder being

penalized if detected.

- It should also be considered that the loss of DOE sensitive information is not the only risk. Remote access provides avenues for a foreign entity into DOE computer systems that could be used to corrupt research data, possibly leading to substantial damage due to incorrect conclusions (if undetected) or, at a minimum, the waste of valuable resources.

There are many controls that could be implemented to mitigate the risk to DOE sensitive information and DOE computer systems. These controls include strong authentication mechanisms for remote users, strong perimeter security controls (e.g., firewalls) to limit the actions of remote users, encryption to ensure intermediaries cannot observe the data in transit, strong access controls on internal DOE systems to minimize the ability for remote users to access data for which they are not authorized, the minimization of provided services on DOE systems to ensure that security flaws in unnecessary programs are not exploitable, and the rigorous application of the latest security updates from commercial system manufacturers to ensure that DOE system configurations are as secure as possible. However, the only truly effective way to prohibit information loss or damage is to simply disallow remote access by foreign nationals.

The recently issued DOE policy on this topic, DOE Notice 205.2, *Foreign National Access to DOE Cyber Systems*, addresses some, but not all, of the counterintelligence concerns regarding remote access to DOE systems by foreign nationals. The recent policy prohibits remote access by foreign nationals directly into systems containing sensitive information (i.e., yellow network systems). However, the granting of access to green network systems provides a malicious

foreign national with the ability to enter yellow network systems through the use of commonly available intrusion techniques. Further, the policy sets no requirements to address the concerns/issues of authentication sharing, spoofing, and hijacking, or the possibility of gaining illegitimate access to computer systems at other DOE sites via legitimate access to one DOE site.

Finally, the Counterintelligence (CI) Cyber Program within OCI is currently working on two activities to address many of these concerns.

- The E-Mail Analysis Capability (EMAC) will attempt to monitor and analyze the information being transmitted by foreign nationals and high-risk personnel to locations outside of the DOE.
- The Inquiry Management and Analysis Capability (IMAC) will deploy consistent intrusion detection capabilities at the external access points to DOE sites. Additionally, IMAC will provide a central analysis facility that will receive intrusion data from all sites and will perform analysis to detect and identify relationships between activities at different sites.

Both of these activities are nearing the point of deployment. The EMAC activity is awaiting the approval of the DOE Office of General Counsel prior to deployment of the necessary hardware and software. The IMAC activity is working to finalize the guiding operational principles that will be used prior to starting deployment of the intrusion detection devices.

Q3. One of the recommendations in your CI plan is for the Secretary of Energy to request that the FBI take over the conduct of background clearance investigations. In the July 1999 Inspector

General (IG) report discussing the status of your plan, it notes that DOE's intention is to have the FBI do only the most sensitive background investigations. You have stated that this recommendation is implemented because the Secretary has made the request, but has the FBI agreed, and are they doing any of the Department's background investigations yet?

A3. The recommendation in question reads as follows:

The team does not believe that Background Investigations (BIs) are being conducted satisfactorily. As such and as per DOE Order 472.1B, *Personnel Security Activities*, and the Atomic Energy Act, as amended, DOE should request that all further Single Scope Background Investigations (SSBIs) be conducted by the FBI.

It remains OCI's view that this recommendation has been implemented, since the Secretary of Energy has requested such assistance from the FBI. The FBI has agreed to conduct 150 reinvestigations in calendar year 2000. Based on the results of those reinvestigations, the FBI will then decide whether it will conduct all SSBIs. OCI believes that this is a reasonable way for the FBI to proceed on this matter.

Q4: Another one of your 46 points is a recommendation to create an expanded Personnel Security Program for high-risk personnel, which would include a polygraph, an expanded financial disclosure form, and a forensic financial investigation. You have stated that this recommendation has been implemented, but when Committee staff spoke with certain lab and DOE field office personnel, they said they saw no evidence of any expanded program. What is the status of this expanded Personnel Security Program, and how many high risk employees have been processed through it to date?

A4: The Personnel Security Program referred to in Recommendation 12 is now the Counterintelligence Evaluation Board (CIEB). The Program Director for CIEB arrived in March 1999, and, in concert with DOE's Program Managers, identified DOE's high-risk programs and positions that require expanded counterintelligence vetting. CIEB has established a counterintelligence polygraph program and is in the process of developing a financial

investigation program. The high-risk programs include Special Access Programs (SAP), the Personnel Security Assurance Program (PSAP), the Personnel Assurance Program (PAP), individuals with access to Sensitive Compartmented Information, individuals who have a need-to-know or access to information regarding the design and operation of nuclear weapons and associated use control features, and individuals assigned to the Offices of Counterintelligence, Independent Oversight and Performance Assurance, and Security and Emergency Operations.

The Secretary of Energy has stated that initially approximately 800 individuals in SAPs, the PSAP and the PAP will receive counterintelligence polygraph examinations. Congress, in Section 3154 of the National Defense Authorization Act for FY2000 (NDAA), has stated that no one will be admitted to a SAP or the PSAP without completing a counterintelligence polygraph examination. DOE estimates that, based upon the NDAA requirement, approximately 1,350 individuals will require initial access to a SAP or the PSAP during CY2000. CIEB has processed more than 200 of these high-risk individuals to date.

Q5. You also have recommended, as part of your CI plan, that the labs make contact with every employee traveling to a sensitive country or having contact with sensitive country foreign nationals in any form, in order to determine whether there are any counterintelligence concerns. In response to questions by this Committee, Livermore described its own program in somewhat different terms, noting that it covered only those employees traveling to a sensitive country, which presumably leaves out other contacts in foreign or domestic locations with sensitive country foreign nationals.

Given that you recently conducted a CI inspection at Livermore, can you describe whether Livermore is meeting the requirements that you laid out in your CI implementation plan on this topic? Are the lab's CI personnel making effective contact with all the traveling employees that they should be? And what about the other labs that your inspection team has reviewed so far?

A5. The answer to this question is combined with the answer to question no. 6 below.

Q6. Livermore also informed the Committee that it had 600 employees travel to sensitive countries last year alone - 425 to Russia and 16 to China. But it has a staff of only a handful of CI officers to handle the required pre-briefs and debriefs from all these trips - officers that have other duties as well. The result is that Livermore must be highly selective in choosing who among these traveling employees it actually will interview in person - with the remainder simply receiving written information requests.

Are you concerned that the labs, despite recent increases, still do not have the resources to run an effective foreign travel program? What are you finding in your CI inspections in this area?

Do you believe that the amount of foreign travel by lab employees to sensitive countries, or to any fora in which they may have contact with foreign nationals from such countries, poses a significant risk to national security? Should the numbers be reduced?

A5 and A6:

The Director, OCI mandated in a memorandum dated 8/30/99 that all hosts of sensitive country foreign nationals and all travelers to sensitive countries be personally debriefed. The following is an accounting of the pre-briefing and debriefing procedures with regard to the interactions of DOE employees with sensitive country foreign nationals followed by each of the laboratories inspected thus far.

LAWRENCE LIVERMORE NATIONAL LABORATORY (LLNL)

The Foreign Visits and Assignments (FV&A) function at LLNL lies outside the direct control and administration of LLNL's CI element, the "Security Awareness For Employees" (SAFE) Program. An Inspection Team visited LLNL from August 9-18, 1999, and assessed that "...The Senior CI Officer (CIO) and his staff have excellent interface with the Foreign Visits and Assignments Office Manager to ensure the tenets of DOE Order 142.1 *Unclassified Foreign Visits and Assignments*, are implemented." The rating of the foreign visits and assignments

program (FV&A) function at LLNL was Satisfactory.²

LLNL CIOs debrief all LLNL employees who have contact with sensitive country foreign nationals. This includes both LLNL employees who travel to sensitive foreign countries and LLNL personnel who host sensitive country foreign nationals. However, the inspection found that LLNL CIOs brief/debrief in person approximately 25% of these people. The remainder receive questionnaires to be completed and returned to the LLNL CI Office. Review of these responses by CIOs may lead to a personal debriefing. Due to the large number of people to be briefed/debriefed (1795 during the period 7/1/98-7/1/99), LLNL CIOs cannot brief/debrief them all in person with the six CIOs onboard at the time of the inspection. The LLNL Senior CIO asked for and received additional CIOs in his funding request for FY00.

The Inspection Team established three Findings and two Recommendations related to FV&A and foreign travel at LLNL:

LLNL CI Inspection Findings

- The LLNL CI Office is unable to track foreign visitor host and foreign traveler debriefing forms to determine whether or not the host or traveler completes and returns the forms to the CI Office.
- With the exception of personnel hosting visitors from China or personnel traveling to

² The rating scale used by the Inspection Team is Excellent, Satisfactory, Marginal, or Unsatisfactory.

China, the CIOs base their decision on whether to interview hosts of foreign nationals, in part, on the information voluntarily provided by the host on a written debriefing form.

- If a host or a foreign traveler does not complete and return the written debrief form, he/she may not be debriefed unless the CIO sets an administrative "tickler" to flag the departure of the foreign visitor or return of the traveler.

LLNL Recommendations

- The Senior CIO should obtain the appropriate computer programming modifications necessary to permit the computer tracking of written debriefing forms.

This action was completed as of February 2000. The software to permit tracking of debriefing forms has been installed and is operational.

- When computer tracking of debriefings forms is available, institute a program to conduct face-to-face debriefings of a significant sampling of those personnel who do not return debriefing forms. These debriefings should be conducted in order to solicit CI information and secure (the interview respondents') future cooperation should they host foreign national visitors in the future.

SAFE will download from its database a monthly list of the people who have not returned their travel debriefing forms. By mid-April, SAFE will get the February report on the

individuals not responding. It then will contact and debrief a sample number of that group. SAFE estimates that many in the non-respondent group may have been debriefed previously. Based on the numbers of those in the reported group who have already been contacted by the SAFE Program, and an assessment of remaining numbers in that group, SAFE management will determine the numbers of debriefings that will constitute a significant sampling, and these individuals will be debriefed in person. The SAFE Program has been provided an additional CI officer in FY 2000, as well as added administrative support to meet the workload.

LOS ALAMOS NATIONAL LABORATORY (LANL)

LANL's CI element, the Internal Security (ISEC) Office, is responsible for the personnel, administration, and management of LANL's FV&A Program. An Inspection Team visited LANL from September 20-30, 1999, and the inspection rating for the FV&A Program at LANL was Marginal.

The Inspection Team was concerned that relative to the FV&A Program, those laboratory personnel assigned to "high risk" programs were not being identified, prioritized or afforded face-to-face interviews by CI personnel. However, according to the Inspection Team, ISEC's FV&A office "...has an effective (local) database in place for tracking foreign visitors/assignees from the point of visit request, initiation, approval or denial, to visit conclusion." In the Spring of 1999, LANL Director John Browne established a Foreign National Working Group (FNWG). The FNWG's purpose is to compile all DOE and laboratory requirements relating to foreign national

access to LANL. ISEC's staff, including the Director, ISEC, participate in some of the FNWG's sub working groups. There were no Findings or Recommendations associated with FV&A at LANL.

OCI determined that access to sensitive programs, such as the Special Access Programs (SAP), had to be addressed at a Headquarters level. This issue now has been resolved to OCI's satisfaction, and each Senior CIO will be granted access to the SAP programs at his or her site. Access to sensitive "work for others" programs or activities funded by other agencies is still in the process of being established as DOE-wide policy. In the meantime, the LANL CI Program has established liaison with the security officers of the SAP, Personnel Assurance Program (PAP), the Personnel Security Assurance Program (PSAP) and Secret Compartmented Information (SCI) programs and developed procedures and policies to address the CI issues for those employees in high risk programs. A CIO has been designated to interface with the security officers for the high risk programs.

LANL's CI Program was reinspected from April 24 to April 30, 2000. The inspection report is not yet in final form.

SANDIA NATIONAL LABORATORIES (SNL - New Mexico and California)

Currently, the Foreign Visits and Assignments (FV&A) process at SNL/New Mexico (SNL/NM) is located in the Safeguards and Security Center. The CI Program - Counterintelligence Awareness Program for Employees (CAPE) -- is located separately. The FV&A is a defined,

well-organized and effective means of administering the foreign visits process from application to departure. Decision-making, which includes the senior CIO having the authority to stop certain visits, is at appropriate levels -- the lab director or his immediate second level managers. An off-site Cooperative Monitoring Center (CMC) keeps most foreign visitors outside SNL/NM secure areas. No foreign nationals have access to any of SNL/NM's supercomputers, and measures are in place to prevent the inadvertent movement of files from classified to unclassified computers.

An Inspection Team visited SNL from October 25 to November 5, 1999, and at that time rated SNL/NM's FV&A Program as Marginal. The Team arrived at the following Findings and Recommendations related to the FV&A Program and to foreign travel at SNL/NM:

SNL/NM Findings

- The SNL/NM CI Office has inadequate plans and resources to meet the mandated requirement to personally pre-brief and debrief all SNL personnel who have sensitive country interactions.

- The SNL/NM CI Office has not developed effective policies and procedures regarding proposed unclassified foreign visits and assignments when indices checks reveal derogatory information.

SNL/NM Recommendations:

- The SNL/NM Senior CIO should immediately initiate a study to determine the extent of the problem attendant to meeting the DOE CI pre-briefing and debriefings requirements. This study should estimate the number of pre-briefings and debriefings required, estimate their complexity and determine the preparation necessary to conduct them competently. An estimate should be made of the additional CIO and administrative support needed. The study should obtain input from SNL/NM divisions and elements associated with visits and assignments and travel in the programs specified in the OCI memorandum.

(Attachment 3 is CAPE's "Counterintelligence Briefings and Debriefings Policy Statement," which was drafted to meet the intent of the briefing/debriefing requirements stipulated in the Counterintelligence Implementation Plan and Director Curran's 30 August 1999 memorandum.)

- The SNL/NM CIO should prepare a request for resources adequate to accomplish the pre-briefings and debriefings and associated tasks, and forward that request promptly to DOE OCI.

Additional resources have been provided to the SNL/NM CI Program. Since the time of the inspection, there are two additional CIO officers on the staff, plus added administrative support. CARDS³ machines have been provided for input of debriefing information into that database, and CARDS training has been provided to the CI Program

³ CARDS (the Counterintelligence Analytical Research Data System) is the classified database maintained by OCI. All DOE CI personnel have access to the database.

staff. Additional CARDS machines will be delivered in the next month. The CAPE program believes it will need additional CIOs to accomplish the required number of pre-briefings, debriefings and associated tasks. A request for additional resources currently is being reviewed by SNL/NM executive management, and DOE/HQ OCI.

- Policies and procedures should be developed to implement the requirements of the 8/30/99 OCI memorandum.

These policies and procedures have been developed, and are under programmatic review. CAPE's internal policy governing the conduct of briefings and debriefings is consistent with the DOE Draft Order for Counterintelligence currently under review at the field level.

- The Senior CIO should develop processes within his office, and reach agreements and understandings with FV&A and other SNL/NM entities that administer, approve, and review sensitive unclassified FV&A. This will expeditiously resolve the equities in FV&A applications that have derogatory indices results to ensure that CI objectives are fully achieved.

C. Paul Robinson, director and President of SNL, and Joan Woodard, Executive Vice President, informed the DOE Inspection Team during the 25 October-5 November 1999 CI Program Inspection that they wished to be notified of all derogatory indices relative to

foreign visits and assignments. This notification ensures that all available information is used in their approval of these foreign interactions at SNL. The SNL Senior CIO developed a formal process with Executive Vice President Woodard for a CAPE CIO, either in person or by secure means, to advise SNL executive management when a particular foreign visitor has a known or suspected affiliation with a foreign intelligence service. The policy further allows for executive management to work with CAPE to determine whether a specific visit should be disallowed or modified.

SNL/NM was reinspected from May 1-5, 2000. The inspection report is not yet in final form.

Sandia/California (SNL/CA):

According to the Inspection, the overall FV&A vetting process at SNL/CA is rated as Effective. The SNL/CA CIO conducts indices checks on all sensitive country foreign nationals visiting or assigned to any area of the site as well as foreign nationals having access to sensitive subjects at the site. The CIO has authority to deny a visit based on derogatory information. All pre-travel briefings and post-travel debriefings are conducted in person. There were no Findings or Recommendations relating to the FV&A program at Sandia/California.

OAK RIDGE NATIONAL LABORATORY (ORNL)

An Inspection Team visited ORNL from January 10-21, 2000, and found that ORNL CIOs and the Oak Ridge Operations Office CIO conduct all required briefings/debriefings in person and enter all required data into CARDS. Due to the large number, some of these briefings are

presented to small groups which is permissible under current OCI directives. These briefings/debriefings were judged by the inspection staff to be very effective. These briefings/debriefings include those conducted by the ORNL CIOs for the other seven facilities which constitute the Oak Ridge complex such as the Y-12 Plant, East Tennessee Technology Park, etc. It should be noted that the ORNL Senior CIO believes that the most effective available CI tool is the briefing/debriefing program.

ARGONNE NATIONAL LABORATORY - EAST (ANL-E)

An Inspection Team visited ANL-E from March 12 - 24, 2000, and found that in CY99, less than half of the ANL-E employees traveling to sensitive foreign countries received in person briefings prior to their travel and only 10% received in person debriefings after their travel. In CY99, there were 1417 visitor/assignee applications from sensitive country foreign nationals. The ANL-E CIO recalls only ten in person host briefings (OCI records indicate 13). The ANL CIO (who is the only person assigned to the ANL-E CI Office) reported that a lack of resources has prevented him from conducting the required briefings/debriefings. The inspection found that he was spending approximately 80% of his time conducting investigations. ANL-E is not meeting the OCI requirements regarding briefings and debriefings. An inspection document was prepared regarding the entire FV&A program at ANL-E, which was found to be not in compliance with DOE Notice 142.1 pertaining to unclassified Foreign Visits and Assignments. Additional CI Office staffing was also recommended by the inspection. ANL-E is in the process of writing an Action Plan setting forth how it will address the recommendations of the Inspection Team, and will be reinspected in September 2000.

PANTEX PLANT

Due to the fact that Pantex is a weapons assembly and disassembly facility, there have been very few foreign visitors from either sensitive or non-sensitive countries. There has never been a foreign assignee. The CI Office briefs and debriefs all employees having interactions with sensitive country foreign nationals.

OCI VIEW ON RISK POSED BY FOREIGN TRAVEL

OCI believes that any DOE employee who travels to a sensitive country, or interacts with a sensitive country foreign national in any other fora, is at risk. However, OCI recognizes that this interaction is often necessary to the ability of DOE to carry out its various missions. OCI believes that the briefing and debriefing requirements it has set forth can effectively manage that risk. While certain DOE facilities are not currently meeting those requirements in full, they are making identifiable progress toward that goal. Over the last six years, funding for DOE's CI Program has increased from less than \$5 million to more than \$40 million, and half of that budget goes to fund the field CI Programs every year. Therefore, these field CI Offices are in a much better position than ever before to meet these requirements, and the inspections are set up to identify when and if additional resources are necessary for them to do so in full.

Q7. Another recommendation in your plan is that CI briefings should be tailored to particular audiences, rather than generalized, particularly with respect to foreign travel by lab scientists and those who host foreign nationals on site. You have stated that this recommendation has been implemented because you instructed the labs to tailor their briefings, but the DOE IG noted in July that you had not yet given the labs sufficient guidance in this area.

Have you now done so, and what did your recent inspections on this issue find? Are the labs now conducting more tailored CI briefings? Are you satisfied?

A7. In July 1999, when the IG conducted their study, OCI had provided no specific guidance to its Field elements on this issue. Since then, OCI has instituted its in-house training program and has hosted two management conferences for its Senior CI Officers (CIOs) from across the DOE Complex. At these conferences, OCI has made clear the need to tailor briefings to scientists going on travel or hosting sensitive country foreign nationals, and the manner in which this customization should be accomplished. More specifically, in the DOE CI Course, which all CI professionals must attend, there is specific training on how to conduct briefings and debriefings within the DOE environment. This training stresses the paramount need to tailor these activities to the target audience. Finally, OCI has integrated this requirement into its training program to ensure that OCI field elements are implementing it.

Q8. In its report on your progress so far, the IG stated that you should give more priority to implementing one of your 46 recommendations dealing with the development of a centralized database for the tracking of foreign visitors and assignees throughout the DOE complex. Have you changed the priority on this recommendation? Can you describe where you are on this recommendation, and how long it will be before it is implemented?

A8. A Department working group chaired by OCI met three times in late 1999 in order to create a comprehensive list of tracking requirements. As a result, the Foreign Access Records Management System (FARMS, the new version of DOE's Visits and Assignments Management System - VAMS) has been modified to address the critical areas of concern raised by the working group. In June 2000, a new centralized automated visits and assignments tracking system will be in place with greatly enhanced features to include connection to local databases, an enhanced report capability, and better inter-operability with existing OCI systems.

Q9: Under DOE's proposed notice on polygraphing, DOE may conduct an investigatory polygraph for cause, provided that the employee requests it in order to exonerate himself. But it

does not appear that DOE would be permitted under this proposed rule to request that someone take a polygraph as part of an investigation, since it is not specifically enumerated as a situation in which a polygraph can take place. Is the intent of this rule to limit the ability of DOE to request a voluntary polygraph in such situations, and if so, why? If not, does DOE plan to amend this notice to make this point more clear?

A9: DOE Notice 472.2, *Use of Polygraph Examinations* was published on March 17, 1999 and states that DOE will administer a polygraph examination to an employee as a means of exculpation in the resolution of counterintelligence investigations or personnel security issues. DOE can suggest that an individual take an exculpatory polygraph examination as a means of resolving counterintelligence investigations or personnel security issues; however, DOE cannot request that an individual submit to such a polygraph examination. This principle has been included in 10 CFR, Parts 709, 710 and 711, *Department of Energy Polygraph Examination Regulation* which replaces DOE Notice 472.2. As with all polygraph examinations administered by the federal government, an individual may decline to take a counterintelligence polygraph examination. DOE does not intend to amend 10 CFR 709, 710 and 711.

Q10: You testified that the actual number of DOE and contractor employees that will be polygraphed under this new program will be determined by the program managers who run the programs at issue. Based on what you have received so far from these managers, can you provide a rough estimate of the number of DOE and contractor employees likely to be polygraphed, complex-wide?

A10: The Program Managers for DOE's eight high-risk programs developed criteria for identifying the positions within their programs that should undergo counterintelligence polygraph testing. Using these criteria the number of DOE employees, federal and contractor, who would undergo counterintelligence polygraph examinations is 2,650 to 3,150.