AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SECURITY AT THE DEPARTMENT OF ENERGY'S LABORATORIES: THE PERSPECTIVE OF THE GENERAL ACCOUNTING OFFICE

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

APRIL 20, 1999

Serial No. 106–31

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
56–604CC WASHINGTON : 1999

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

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

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

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

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

FRED UPTON, Michigan, *Chairman*

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

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

CONTENTS

Page

Testimony of:
Rezendes, Victor S., Director, Energy, Resources, and Science Issues; accompanied by John Schulze, Assistant Director, Energy, Resources, and Science Issues; William Fenzel, Assistant Director, Energy, Resources, and Science Issues; and Gary Boss, Assistant Director, Energy, Resources, and Science Issues, General Accounting Office 17

SECURITY AT THE DEPARTMENT OF ENERGY'S LABORATORIES: THE PERSPECTIVE OF THE GENERAL ACCOUNTING OFFICE

APRIL 20, 1999

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

The subcommittee met, pursuant to notice, at 2 p.m., in room 2322, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Burr, Bilbray, Bliley (ex officio), Klink, Stupak, and Dingell (ex officio).

Also present: Representative Wilson.

Staff present: Tom Dilenge, majority counsel; Jan Faiks, majority counsel; Jason L. Foster, legislative clerk, and Edith Holleman, minority counsel.

Mr. UPTON. It's 2 o'clock, we're going to begin the hearing. I know a number of members are scattered all over the place, and they will be here and back a few times. In the interest of time, and in the interest of a very important meeting on another important topic to the country, and certainly to Michigan, the nuclear waste bill, there is a meeting between Mr. Bliley and Mr. Dingell that is supposed to take place at 2 o'clock, and since both members are here and it is after 2 o'clock, I am going to let them give the opening statements. Mr. Bliley.

Chairman BLILEY. Thank you, Mr. Chairman. Our committee has jurisdiction over the operations and management of the Department, including its privately run laboratories. Over the past two decades, this committee has taken a strong bipartisan interest in ensuring that the Department's laboratories maintained effective security systems, and that the Department's internal security reviews offer timely and candid assessments of the status of safeguards at particular sites.

Unfortunately, the Department's history in this area can most charitably be characterized as spotty at best. The historical pattern is clear, internal Department criticism on security matters either gets dismissed or white-washed until some event crystalizes public attention—which in turn leads to a flurry of reform initiatives that sound great in theory but falter against the reality of the DOE bureaucracy. And once public attention has shifted to some other topic—as it inevitably does—the Department returns to business as usual.

The written testimony that we have received today from the General Accounting Office makes this point all too clear. A perfect example is the Department's response to criticism in 1988 that its nuclear weapons laboratories were not conducting adequate background checks and other counterintelligence activities with respect to foreign visitors from sensitive countries such as China. DOE agreed to increase background checks on such visitors and brought in agents from the Federal Bureau of Investigation as detailees to help improve counterintelligence at the labs. However, in 1994, the Department granted waivers from the background check mandate to two of its most sensitive weapons labs. Around the same time, the FBI pulled its agents out of the Department because it believed that their views and recommendations on counterintelligence were not being taken seriously by managers at the labs and at DOE headquarters.

Not surprisingly, when GAO returned to this topic in 1997, it found that the foreign visitor situation at these two labs had only gotten worse, despite all the promises of reform back in 1988. GAO notes in its testimony today that the current Chinese espionage scandal has spawned similar promises of reform—increased background checks and FBI systems with counter-intelligence. But until we address the underlying causes of the Department's systematic security failures, I feel we may be doomed to repeat history's mistakes.

I also am troubled by the repeated suggestions that the recent spy charges are old news—isolated, historical events that occurred on some other administration's watch and could not occur today because of new security measures put in place. I believe the testimony this afternoon will shed considerable doubt upon those claims, which demonstrate a marked arrogance and ignorance of both history and current events. As GAO will discuss this afternoon, security problems—particularly in the area of computer security—continue to persist unresolved, even today, posing a significant threat to our Nation's most prized secrets.

While no system can ever be fail-safe, the American people deserve better than this. I hope that the bipartisanship that was present when we looked at past administration activities in this area will not suffer as we begin, along with GAO, to look more closely at the current state of security at the Department's sensitive facility.

Thank you, Mr. Chairman.

Mr. UPTON. Thank you, Mr. Chairman. Mr. Dingell.

Mr. DINGELL. Mr. Chairman, thank you.

I would commend you for holding this hearing, and I want it to be noted that I am very pleased to see that this subcommittee is, once again, taking up the very important and challenging issue of security and safeguards at our country's nuclear weapons laboratories. This is a matter into which this committee has been going, both during the time that I have been chairman and the time that you have been chairman, and the time that others have presided over the business of the committee, to ascertain what is transpiring with regards to safety and security at these nuclear facilities. This subcommittee and this committee have a long and proud history of bipartisan work on this issue.

I have, attached to my statement, a letter detailing the committee's previous work on unclassified matters, that I sent to former Senator Warren Rudman, who was charged by President Clinton to look at the security of these labs. Today's hearings will not address classified matters; but, I know that the committee's previous attention to these matters was quite sweeping, and did address a number of matters of serious concern to the country.

As you know, Mr. Chairman, the safeguards and security problems at the Department of Energy has spanned five different administrations, at least eight Energy Secretaries, the cold war, the end of the cold war, the era of non-proliferation, and the new era of emerging nuclear powers. We cannot lay the blame of these shortcomings as the fleet of any one President, or any one Energy Secretary. We know, from personal experience on this committee, that despite talk of personal terrorism, or rather potential terrorism, each President and almost all Energy Secretaries have responded inadequately to both external and internal warnings; that all was not well. Many of those warnings have come, I would note, from this subcommittee over the years, and the period during which those warnings have come has exceeded at least 10 years, and perhaps more. None of the Secretaries, and none of the Presidents, gave the security operations staffing or the funding that it needed to protect our most secret weapons facilities. Negative evaluations were buried. Whistleblowers were punished. And private contractors, which actually ran the labs, and are employers of all the lab staff, often refused to make changes to improve security at their facilities, in defiance of Department of Energy mandates and warnings of this subcommittee. Scientists are not trained to understand how they might be targeted, and how they might be solicited, as sources of secret information. The labs had no counterintelligence operation, because funding of such an undertaking would take money away from program funds.

This subcommittee found out, in 1982 and 1989, that protecting its sensitive nuclear weapons facilities is not a high priority at DOE, then, or now. In 1981, when this subcommittee began its formal investigation into safeguards and securities at the labs, with the assistance of the General Accounting Office—and by the way, I want to observe, Mr. Rezendes, and your associates, we appreciate the good work you did then on this matter, and on a number of other of other matters—that our weapon facilities were potential and vulnerable targets for state-sponsored and other terrorists.

As a result, this subcommittee, the General Accounting Office, and the internal Department of Energy reports often focused on shortcomings in physical security and related management problems that allowed them to continue. A long series of GAO reports was done for this committee and for this subcommittee, or for the Senate Governmental Affairs Committee, under the leadership of our former colleague, Senator John Glenn.

By the late 1980's, Congress was also looking at the interaction of our scientists with foreign scientists, through the foreign visitors' programs. Numerous security violations in that program were uncovered, which remained unaddressed when the GAO began to look at it again in 1997.

The security of the computer systems and the problems with the counterintelligence operation were other important areas in which GAO raised serious concerns. I am encouraged that Secretary Richardson has responded quickly in addressing allegations of espionage, creating our lab scientists to recognize and withstand attempts by foreign interests, use them as sources of critical information, as essential for the long-term security of this country, as is the understanding and strengthening of the labs' computer system. But we know from past experience that aggressive and continued congressional oversight is needed to fix these problems, after the crisis and news headlines have passed.

I hope, Mr. Chairman, that this subcommittee will take up the task again. I look forward to working with you, and cooperating with you, in the same bipartisan fashion we have done in times past, when we have addressed these matters. And I am hopeful at this time we will have better success, in terms of dealing with yet another administration that has not done the kind of job that it should have done, in terms of dealing with security at major weapons and defense facilities.

I thank you for recognizing me, Mr. Chairman.

[The prepared statement of Hon. John D. Dingell follows:]

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

Mr. Chairman, I am very pleased to see that this Committee, once again, is taking up the very important and challenging issue of security and safeguards at our country's nuclear weapons laboratories. We have a long and proud history of bipartisan work on this issue. I have attached to my statement a letter detailing the Committee's previous work on unclassified matters that I sent to Warren Rudman, who was charged by President Clinton to look at security at the labs. Today's hearing will not address classified matters, but I note this Committee's previous attention to those matters as well.

As you know, Mr. Chairman, safeguards and security problems at the Department of Energy have spanned five different administrations, at least eight Energy secretaries, the Cold War, the end of the Cold War, and the era of nonproliferation and new, emerging nuclear powers. We cannot lay the blame for these shortcomings at the feet of any one President or any one Energy Secretary. We know from personal experience that—despite all talk of potential terrorism—each President and almost all Energy secretaries have responded inadequately to both external and internal warnings that all was not well.

None of them gave the security operation the staffing or funding it needed to protect our most secret weapons facilities. Negative evaluations were buried; and whistle blowers punished. The private contractors, which actually run the labs and are the employers of all of the lab staff, often refused to make changes to improve security at their facilities in defiance of Department of Energy mandates. Scientists were not trained to understand how they might be targeted and solicited as sources of secret information. The labs had no counter-intelligence operation because funding it would take away from program funds. This Subcommittee found in 1982 and 1989 that protecting its sensitive nuclear weapons facilities was not a high priority for DOE.

In 1981, when this Subcommittee began its first formal investigation into safeguards and securities at the labs—with the assistance of the General Accounting Office—our weapons facilities were potential, and vulnerable, targets for state-sponsored and other terrorists. As a result, we, the General Accounting Office, and internal Department of Energy reports often focused on shortcomings in physical security, and related management problems that allowed them to continue. A long series of GAO reports was done for this Committee or for the Senate Governmental Affairs Committee, under the leadership of John Glenn.

By the late 1980s, Congress was also looking at the interactions of our scientists with foreign scientists through the foreign visitors programs. Numerous security violations in that program were uncovered which remained unaddressed when GAO looked at it again in 1997. The security of the computer systems and problems in

the counterintelligence operation were other important areas in which GAO raised concerns.

I am encouraged by Secretary Richardson's quick action in response to the latest allegations of espionage. Training our lab scientists to recognize and withstand attempts by foreign interests to use them as sources of critical information is essential to our long-term security, as is understanding and strengthening security of the labs' computer system. But we know from past experience that aggressive and continuous Congressional oversight is needed to fix these problems after the crisis and the news headlines have passed. I hope, Mr. Chairman, that this Committee will take up that task again.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON COMMERCE
March 24, 1999

The HONORABLE WARREN RUDMAN
President's Foreign Intelligence Advisory Board
Room 340, Old Executive Office Building
Washington, D.C. 20502

DEAR WARREN: First, let me congratulate you on your recent appointment to lead the bipartisan review of security threats to the U.S. nuclear weapons laboratories over the last twenty years. I am hopeful that your review will finally focus appropriate attention on a very serious and longstanding problem that has been ignored, mismanaged, and/or covered up during several Administrations. Unfortunately, your effort is only the latest in a long line of reviews undertaken by, among others, the General Accounting Office (GAO), the Department of Energy (DOE) and its Inspector General, the U.S. Nuclear Command and Control System Support Staff, and various Congressional committees, the results of which have been uniformly ignored by the responsible officials.

I am also writing to offer you my assistance as you undertake this review. During my 14-year tenure as chairman, the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce conducted several classified and unclassified inquiries into this matter. (This letter discusses the unclassified portion of our work.) We found a disturbing pattern of security weaknesses in the contractor-run national weapons laboratories, along with extraordinarily lax oversight by the Department of Energy (DOE). As you may already know, these problems included: laboratories refusing to implement basic security precautions; DOE Secretaries and other officials ignoring repeated warnings of security problems; and bureaucratic obfuscation of the problems that meant that even the National Security Council and the President received inaccurate, misleading information. Although our main focus initially was terrorism and physical security, our concerns soon broadened to encompass other significant security deficiencies and the system's management problems.

The Subcommittee, on a bipartisan basis, sought continuously to bring these problems to light, and to fix the underlying weaknesses, such as the lack of independent security oversight, that allowed problems to persist. This work required a sustained effort over several years, work made more difficult because of the recalcitrance of the contractors running the national laboratories. You should expect significant difficulties in arriving at a full understanding of the problems, particularly if, given your tight deadline, you are forced to rely on those contractors and government officials responsible for managing the laboratories over the last twenty years.

The Subcommittee's work on this matter began in 1981 in response to efforts to undermine independent review of security threats. The Department of Energy's Assistant Secretary of Energy for Defense Programs had become concerned in 1979 about the level of security at the weapons laboratories. As recommended by the General Accounting Office (GAO) in 1977, and also the Inspector General, he established an independent, inter-agency group that reported directly to him on the adequacy of safeguards at these facilities. This program employed some of the best experts in the country in terrorism, sabotage, protection of classified material and related activities. This group found that the safeguards at the most critical facilities—which included Los Alamos—were in shambles while, at the same time, DOE's Office of Safeguards and Security was giving the facilities a clean bill of health.

However, in 1981, when a new Administration took over, the Assistant Secretary was replaced by a high-ranking official from Los Alamos National Laboratory who immediately shut down the independent assessments program. In 1982, in a classified report to the Subcommittee, GAO strongly recommended (in part because DOE was submitting misleading reports to the National Security Council) the reinstitution of an independent assessment program which would report directly to the

Under Secretary of the DOE. Two hearings by the Subcommittee in 1982 and 1983 focused on the organizational problems at DOE and the GAO recommendation. In 1983, the Committee adopted, with strong bipartisan support, an amendment to the DOE Defense Authorization bill establishing an independent Office of Safeguards Evaluation reporting directly to the Secretary. Unfortunately, the bill never received floor consideration.

Attempts by the Subcommittee and others in 1983-84 to establish an independent evaluations office within DOE were turned down by the Secretary and the Assistant Secretary for Defense Programs, who wanted the evaluations program under his control. Independence was critical because, during the Subcommittee's work, top officials misled the Subcommittee and harassed a DOE whistleblower. In 1984, the Subcommittee held a hearing on the Department's attempts to strip the employee's security clearance and issued a report. The Department rewarded the harassers with promotions, bonuses and medals. In 1984, the Department also terminated an investigation by its Inspector General into management adequacy in the safeguards and security program.

The Subcommittee also attempted to alert President Reagan to its concerns. In 1984, however, DOE officials told the President there was nothing to be concerned about. In January 1986, prior to his briefing by DOE on the status of safeguards and security, I wrote a letter to President Reagan listing general problem areas. These included: credibility of the inspection and evaluation program; inadequately trained guard forces; inadequate protection against insider threats; inability to track and recover special nuclear materials and weapons if they were stolen; inadequate protection of classified information; inverse reward and punishment system for the contractors; and lack of funding for safeguards and security upgrades. (A copy of that letter is enclosed.) In response, based on information provided by the national laboratories and DOE officials, Secretary of Energy Herrington wrote of "significant progress" and "improvements," and Admiral Poindexter said he was "impressed with the progress being made."

The Subcommittee continued its work during President Bush's Administration. Among other matters, it looked at inadequate personnel security clearance practices at the laboratories where it was immediately clear that there were inadequate resources to do an effective job. That situation has not changed to this day. The Subcommittee also began to review the foreign visitors program—as did Senator Glenn, then chair of the Senate Governmental Affairs Committee—and the mysterious shutdown of an investigation into drug problems and property controls at Lawrence Livermore Laboratory.

At the same time, Secretary Watkins' Safeguards and Security Task Force recommended establishing independent oversight functions which would report directly to the Under Secretary. Once again, the recommendation was not implemented, although Secretary Watkins did move the Office of Security Evaluation out from under Defense Programs.

In 1991, the Subcommittee also reviewed the role the Department may have played in allowing Iraq to augment its nuclear capability. In May of 1989, DOE employees attempted to alert Secretary Watkins to the fact that Iraq was shopping for strategic nuclear technologies. They were not allowed to brief the Secretary. But in August of 1989, three Iraqi scientists attended the "Ninth Symposium (International) on Detonation" sponsored by the three weapons labs, the Army, Navy, and the Air Force. It was described by a DOE official as the place to be "if you were a potential nuclear weapons proliferant." At the time, DOE didn't even have a nonproliferation policy, and Secretary Watkins was not briefed on the Iraqi threat until May of 1990.

In 1991 and 1992, the Subcommittee received six GAO reports critical of DOE's safeguards and security efforts. These covered weaknesses in correcting discovered deficiencies, incomplete safeguards and security plans, weak internal controls, unreliable data on remedial efforts, inadequate accountability for classified documents, and security force weaknesses. Two other GAO reports noted that even basic control measures for non-classified property were not in place at the Lawrence Livermore National Laboratory, nor was DOE oversight adequate.

Subcommittee staff met with Secretary O'Leary and her senior staff in 1993 to outline these concerns. At the time of the Republican takeover of the House in January 1995, when my chairmanship ended, the problems had not gone away, and recent GAO reports find little, if any, improvements. In March of 1998, the U.S. Nuclear Command and Control System Support Staff, an independent, federal-level organization chartered by Presidential Directive to assess and monitor all equipment, facilities, communications, personnel and procedures used by the federal government in support of nuclear weapons operations, recommended once again a high-level, independent office to review safeguards and security at DOE.

Many of us in the Congress have tried for years to address the chronic problems at DOE's national laboratories. You now have the opportunity to take an independent, comprehensive, and bipartisan look at these security weaknesses. Independence from those who have failed to solve these problems—which includes officials at DOE and representatives of the laboratory contractors who implement and establish policies at the labs as if they are academic researchers, not the guardians of our weapons secrets—is essential for your review to accomplish more than the prior reviews. Similarly, the independence of any future evaluations office will be essential to any lasting progress.

Your review will not be easy work, but I stand ready to help.

With every good wish.

Sincerely,

JOHN D. DINGELL
Ranking Member

Enclosures
cc: The Honorable Tom Bliley, Chairman
Committee on Commerce
The Honorable Bill Richardson, Secretary
U.S. Department of Energy

U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
January 28, 1986

The HONORABLE RONALD W. REAGAN
President of the United States
The White House
Washington, D.C. 20500

DEAR MR. PRESIDENT: The Subcommittee on Oversight and Investigations understands that you will soon be briefed by senior officials of the Department of Energy (DOE) on the adequacy of safeguards and security at DOE nuclear weapons facilities. The Subcommittee had been conducting an extensive review into the adequacy of DOE's safeguards and security program since mid-1982. On several occasions, I have written to you about the Subcommittee's concerns. The Subcommittee staff has also briefed the staff of the National Security Council and several members of the Council's staff have attended our closed hearings.

While many improvements have been made, serious vulnerabilities remain. Compounding this problem are unresolved management issues and a lack of confidence in the Department's Inspection and Evaluation function which is supposed to provide independent, credible assurances as to the adequacy of safeguards and security. The Subcommittee will be holding a closed hearing in the near future concerning those issues and others. We will notify the National Security Council of the date of our upcoming hearing.

You have said many tines that America will not be held hostage to terrorism. You advocate strong actions to curb this threat to the safety of not only the American people, but to the international community as well. While strong measures against terrorism are absolutely essential, we should also be doing the best job possible to protect our domestic nuclear weapons production facilities from the catastrophic consequences of a terrorist attack.

Unfortunately, the Subcommittee has found that serious safeguards and security vulnerabilities continue to exist at some DOE nuclear weapons sites. The DOE's own internal inspection reports show that plutonium and highly enriched uranium are still highly vulnerable to theft and sabotage at these locations. In meetings with the Subcommittee staff, DOE officials seemed unaware of many of these vulnerabilities. The Subcommittee will continue its vigorous oversight over this critical program until the Department is doing an adequate job to protect the nation's nuclear weapons complex.

The following are several generic problem areas that the committee believes must be resolved in order to have an effective safeguards and security program and which you may want to insure are addressed in your DOE briefing:

Credibility of the DOE's Inspection and Evaluation program—The Subcommittee has evidence that Inspection and Evaluation personnel altered ratings on inspections of safeguards and security interests having important national security significance. The rating system which is used is highly misleading.

Guards forces are inadequately trained—In one exercise using sophisticated testing apparatus known as MILES equipment, the mock terrorists were able to steal plutonium because of a bizarre sequence of blunders on the part of the guard force. One machine gunner had not been trained to load his weapon. Another guard's machine gun jammed and he was not able to unjam it because he had not been trained adequately. A helicopter was dispatched to chase the escaping terrorists. The guards, however, were unable to fire on the terrorists because they had forgotten to bring their weapons. The terrorists disappeared into the woods. This is a contractor guard force that is paid $40 million to guard this critical site. This same guard force has lost M-16 rifles, has refused to allow guards to carry loaded M-16 rifles and shotguns, and has even defied DOE authority, yet received $762,400 in an award fee in 1985 for "excellent" performance.

Inadequate protection against insider threat—During a recent exercise at one of our most critical facilities, an insider was able to smuggle a pistol, with a silencer, and explosives into the facility to be used several days later in a successful attempt to steal bomb parts containing plutonium.

Use of deadly force by security guards.—There is a conflict with state law in some states over whether deadly force can be used to prevent the theft of Special Nuclear Materials. The DOE has been "studying" this matter since it was raised in our September hearing. It is not resolved and, therefore, is a continuing serious weakness.

Lack of coordination with the military, other Federal agencies and local law enforcement for external assistance in the event of an attack—At a subcommittee hearing in September 1982, concern was raised over the failure of the DOE to provide for proper outside assistance. This issue is far from resolved.

Inability to track and recover Special Nuclear Material and nuclear weapons in the event they are stolen from the DOE.—The Subcommittee believes major problems exist. In a recent test, the mock terrorists successfully stole plutonium bomb parts and disappeared. DOE officials admit they would have had a very low probability of locating the terrorists or the bomb parts. To our knowledge, this capability has never been adequately tested.

The Department's inverse rewards and punishment system—The DOE continues to promote and reward officials who have been responsible for safeguards and security problems, including the misleading of the President and the Congress, while holding back the careers of those employees who have tried to improve safeguards and security and to insure that the President and Congress are properly advised of major safeguards and security deficiencies.

Inadequate protection of classified information—The DOE has lost seven sensitive TOP SECRET documents that, to our knowledge, have not been located. Computer systems are vulnerable to compromising highly sensitive, classified data in some DOE locations.

Reduction of funds for safeguards and security upgrades—While the DOE has historically thrown money at its problems, there are essential safeguards and security programs that must be funded adequately. It is important that safeguards and security effectiveness not be hurt due to lack of adequate funding.

We both want adequate protection at these critical facilities. I hope that these concerns will be helpful in your efforts to insure that proper security throughout the nuclear weapons complex does indeed become a reality. Please inform the Subcommittee of your observations after receiving your briefing.

The Subcommittee and its staff will be pleased to assist you and the National Security Council in any way we can.

Sincerely,

JOHN D. DINGELL, *Chairman*
Subcommittee on Oversight and Investigations

cc: Vice Admiral John M. Poindexter
Assistant to the President for National Security Affairs

Mr. UPTON. Thank you, Mr. Dingell. And I thank both you, and the chairman of the committee, Mr. Bliley, our two senior members in the committee, for their insight and their participation this morning.

We are here today to begin what I expect will be a series of hearings on the status of safeguards and security at the Department of Energy's nuclear weapons facilities, and in particular, its privately

run laboratories, which conduct this Nation's most highly sensitive nuclear weapon-related research.

We've all heard a great deal recently about the very serious allegations of Chinese espionage at DOE's nuclear weapons labs. What we'll hear today is that none of these troubling events should have come as any surprise to us, given the long history of significant deficiencies in various aspects of DOE's security apparatus.

While a review of the written testimony for this hearing quickly reveals an incredible breadth of topics that can and should be explored, I must say that one particular area stands out in my mind—the fact that thousands of foreign scientists from countries such as China, Cuba, Iran, and Iraq, are permitted to visit our most sensitive weapon laboratories, and have fairly unrestricted exchanges with our scientists, including those working on matters that, while technically unclassified, are immensely useful for the weapons programs of foreign nations with potentially hostile intent toward the United States or its friends and allies around the world. China alone, sent nearly 1,500 scientists—including suspected intelligence agents—to our three most sensitive weapon labs during the time period of 1994-1996, and according to the testimony we will receive today, less the 2 percent of those Chinese scientists received any background checks at all by the Department of Energy.

But my concern goes beyond the mere fact of whether the Department conducts an adequate background investigation on these foreign scientists. My concern goes to the very heart of this particular arrangement, and whether we are doing all that we should to give counter-intelligence training to those American scientists who must interact with foreign scientists, either here or abroad.

Our witnesses today are from the GAO, and collectively, they have spent decades critically analyzing DOE's security systems and recommending much-needed improvements along the way. I am glad to have them here for the kickoff hearing on laboratory security, to give their perspective of some of the key factors underlying the general inability of the Department to get a firm and permanent handle on safeguards and security at its sensitive nuclear-weapons facilities.

Our purpose today is mostly education—to help Members of Congress and the public put the current spy scandals in a broader, historical context. I should point out that the GAO is currently conducting, at this committee's request, a comprehensive update of its key security work—and the work of other experts within and outside the Department in this area—and will report back to us sometime later this year with a more current assessment of the Department's safeguards and securities.

I also wanted to compliment the witnesses for getting their joint testimony to the committee in a timely fashion—something that is, unfortunately, increasingly rare. Timely written testimony really does help the Congress do its job, and makes these hearing much more useful and effective for both members and the general public.

And I said from the start, I would hope to continue this hearing in the not-to-distant future with other witnesses from the Department of Energy, in its laboratories, so that we can fully explore this important topic.

I yield to my friend and the ranking member of this subcommittee, Mr. Klink from Pennsylvania.

Mr. KLINK. Mr. Chairman, I thank you. I just want to start off by associating myself with the concerns that you stated in your opening statement. I think one of the most difficult problems that this committee has had to face over the last several decades is making sure that the Department of Energy has effective safeguards and security programs at the nuclear weapons plants and laboratories.

In the 1980's, the Oversight and Investigations Subcommittee held numerous classified and unclassified hearings to attempt to correct the often shocking lapses of security at the weapons facilities. Although improvements were made, it was slow and difficult work. Many of these changes involved physical security, in what we often refer to as gate, guards, and guns. But by the early 1990's, the challenge had changed, and meeting the challenge was much more difficult. It involved ensuring secure information systems, and training researchers on espionage tactics of persons who are seeking nuclear weapons, in an era of increased openness and non-proliferation, which encouraged scientific interaction.

In the past, DOE management never provided the leadership, commitment, and resources necessary to address many of the problems. And the contractors who actually run the facilities often were recalcitrant. The labs, in particular, have been worlds unto themselves. The public and the media consider the lab employees, such as those at Los Alamos, to be DOE employees. They actually work for, and are accountable to, private contractors. For example, former DOE, under Secretary Charles Curtis, testified before the Senate Armed Service Committee recently that the labs refused to carry out his security directives. Security training for the scientists, who are the logical target for espionage, totaled 1 to 2 hours per year, and focused on physical security. The subcommittee staff was told just yesterday, of a deputy laboratory director, who, when confronted by DOE with a computer security problem, said he was willing to take the risk of penetration of the system, rather then improve the security.

The new lab director at Los Alamos is attempting to change that. Last fall, he initiated security standdown days, during which different offices take the day off to focus on security issues. He also has required senior lab management to participate in the security training, which may be the first time that these people have appeared in such training. And a few weeks ago, Secretary Richardson shut down the computers in order for the scientists to attend a week's worth of training.

Mr. Chairman, I just received, a few moments ago, a letter to Chairman Bliley from Secretary Richardson. The attachments to that letter were secret; we have not received the attachments. I assume that, at some point, that we will be able to share those with you. It says, when separated from the attachment, handle this document as unclassified; I'm referring to the letter, the unclassified portion. I would ask, Mr. Chairman, if the letter from Mr. Richardson, minus the secret added attachments, might be made a part of this record?

Mr. UPTON. Without objection.

[The letter follows:]

THE SECRETARY OF ENERGY
Washington, DC 20585

THE HONORABLE TOM BLILEY
Chairman
Committee on Commerce
U.S. House of Representatives
Washington, DC 20515-6115

DEAR CHAIRMAN BLILEY: Thank you for your correspondence of March 23, 1999, regarding the Department of Energy's (DOE) Safeguards and Security Program. I want to assure you that the Department will cooperate fully with the Committee on Commerce examination of the overall status of the program. We will also cooperate in the broader review which you have requested be conducted by the General Accounting Office.

In your letter you expressed concern over the long history of unresolved DOE security problems. In all candor, since assuming my responsibilities as Secretary of Energy, I have also become increasingly concerned over these longstanding problems and have initiated aggressive steps to correct them.

Specifically, we have augmented security at field sites by deploying new technologies to safeguard special nuclear materials and weapons; worked with other agencies to train departmental protective forces; identified and developed more sophisticated detection and deterrent systems; and hired additional security personnel. Additionally, we are installing new explosive detection systems at selected nuclear facilities and upgrading our access control systems.

In the area of information security, I recently announced a sweeping cyber-information security program. As part of this program, I also directed the stand-down of classified computer operations at three of our National Laboratories for twelve days, until I was assured that information processed on the systems are being adequately protected. This program also includes computer security and threat awareness training, physical modification to computer equipment to prevent classified information being moved to unclassified systems, new procedures and personnel security requirements for classified file transfers, and installation of automated monitoring systems to scan unclassified archives and e-mail. The program will also require more stringent application of need-to-know criteria and access policies, and initiation of technical measures to increase network security against insider threats. In addition, the three laboratories will rapidly complete unclassified network protection programs to prevent disclosure of unclassified but sensitive information. Finally, each lab will institute information security vulnerability analyses (red teams) and senior technical computer policy boards. Please find attached the Tri-Lab INFOSEC Action Items Proposal submitted by the Laboratories for more details concerning this program.

The Department has also requested a dramatic increase in its budget for information security. The additional funding will be used to help further secure classified and unclassified computer networks throughout the Department. The improvements will help strengthen fire walls, develop additional intrusion detection devices, and fund rapid response teams to work with the FBI to detect and track cyber intruders. The improvements will also allow for even greater security in the Department's unclassified e-mail systems and strengthen protection of the classified computer systems.

The Department has also established the Fissile Materials Assurance Working Group (FMAWG), to assess needed areas of improvement and make recommendations regarding control, measurement and accountability of special nuclear materials. The FMAWG has been successful in identifying unmeasured materials and initiating actions to resolve discrepancies. The working group has also identified additional issues regarding the safeguarding of irradiated material and we are promulgating programmatic direction for implementation. In addition, the Department has developed a standard computerized nuclear materials accounting system that is being implemented at numerous field sites. Finally, we are developing new technologies for tamper-indicating devices and proposing pilot projects for field implementation.

In your letter you also noted that you are troubled by DOE's continuing failure to implement expert recommendations made repeatedly over the last decade, and your concern regarding a lack of accountability concerning the Department's security problems.

It is true that numerous external and internal reviews have raised issues concerning roles and responsibilities and accountability within the Department's Safeguards

and Security Program. Accordingly, I have directed the DOE Security Council to examine our current structure, identify organizational impediments, and formulate a course for corrective action. Specific attention will be directed at policy development and implementation, program planning and direction, accountability, and oversight.

In addition, the Department's site security planning process has been revised and considerably streamlined. Actions include issuing a revised security plan format and content guide and an Acceptance Criteria and Review Guide. Finally, DOE recently clarified the roles and responsibilities of the headquarters and field elements engaged in security planning.

You also raised a concern over reports of unregulated exchanges and visits with foreign scientists in your letter. In this regard, considerable effort is underway to revamp our foreign visits and assignments program. Specifically, a new foreign visits policy has been prepared and is undergoing final review. An improved capability is being developed for documenting information about foreign visitors. In addition, security training is currently underway to educate personnel on intelligence gathering activities of foreign interests.

In addition, I have taken a number of initiatives to strengthen the Department's Counterintelligence programs including increasing the budget to $40 million (from $2.6 in 1995). We have one of the country's foremost counterintelligence professionals, Ed Curran, a 35 year FBI veteran, leading our efforts in this area. Mr. Curran reports directly to me and the counterintelligence personnel assigned to our laboratories report directly to him, as well as to the Lab directors. Furthermore, we have initiated a Department-wide polygraph program to weed out potential counterintelligence problems. Passing a counterintelligence polygraph will now be a condition for entry into DOE's most sensitive programs. These initiatives are covered in greater detail in the Department's Counterintelligence Plan which is provided as an attachment.

I believe the measures outlined above will significantly improve the Department's security posture in the near term as well as in the future. As an indicator of my determination to achieve concrete improvements, I have established a goal of satisfactory ratings for the three facilities rated marginal in the 1997-1998 Annual Report to the President on the Status of Safeguards and Security at Department of Energy Nuclear Weapons Facilities: Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and the Transportation Safeguards Division. I assure you I intend to hold the management of these activities accountable for undertaking corrective actions and achieving satisfactory overall ratings by the end of calendar year 1999.

To facilitate committee staff interviews with laboratory directors and security officials within the Department, I have designated Mr. Joseph Mahaley, Director, Office of Security Affairs, as the primary point of contact. Mr. Mahaley has been instructed to assist committee staff personnel in the collection of all requested information and the scheduling of requested interviews. He may be reached at (202) 586-6591.

Again, I want to assure you the full support of the Department of Energy as the Congress and the General Accounting Office commence their respective reviews. I am fully committed to ensuring the protection of the national security assets entrusted to this Department. In the interim, should you have any other requests concerning this issue, please contact me or have your staff contact Mr. Mahaley.

Yours sincerely,

Bill Richardson

Attachments

cc: The Honorable John D. Dingell, Ranking Member
The Honorable Fred Upton, Chairman,
Subcommittee on Oversight and Investigations
The Honorable Ron Klink, Ranking Member,
Subcommittee on Oversight and Investigations

Mr. KLINK. Let me just say that what Secretary Richardson has laid out is a good start, but I agree with the chairman. We have to continue to have questions about whether the site-specific security and the safeguards plans up-to-date are going to be enough. We wonder if the Department has an accurate overall threat assessment, and site-specific vulnerability assessments, so that it is spending the money in the right place.

Now, the President said he would like $40 million for counterintelligence at DOE. That is encouraging, but I might also add it

represents an enormous budget increase, and we in Congress must make sure that this money can be used effectively. When the General Accounting Office tracked an earlier appropriation that Congress made specific for counterintelligence, it found that most of the money ended up in headquarters studies and excessive overhead charged by the individual facility. In fact, several facilities reduced the amount of money that they allocated to counterintelligence. We must make sure this does not happen in this instance. If we are going to come up with this money, we have to make sure it is used effectively, and I believe, Mr. Chairman, that the oversight investigation of this subcommittee can do that.

The two labs implicated in the most recent allegations, took the most in overhead. We do not want that to happen again. We need to take a close look at this request, and make sure we are fixing problem, not just throwing money in it. Mr. Chairman, the subcommittee has traditionally had all the endurance it took to review safeguards and securities at these facilities, long after the press moves on. I look forward to participating in the oversight of these weapons facilities and labs by this subcommittee, and I congratulate you on your leadership and look forward to working with you in a bipartisan fashion, so that we make sure that the security is as much as it can be at these facilities.

[The prepared statement of Hon. Ron Klink follows:]

PREPARED STATEMENT OF HON. RON KLINK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

One of the most difficult problems this Committee has faced over the last several decades is making sure that the Department of Energy has an effective safeguards and securities program at its nuclear weapons plants and laboratories. In the 1980s, the Oversight & Investigations Subcommittee held numerous unclassified and classified hearings to attempt to correct the often shocking lapses of security at the weapons facilities. Although improvements were made, it was slow and difficult work. Many of these changes involved physical security, or what is often called "gates, guards and guns." By the early 1990s, however, the challenge had changed and meeting it was much more difficult. It involved assuring secure information systems and training researchers on the espionage tactics of persons seeking nuclear weapons in an era of openness and nonproliferation which encouraged scientific interactions.

In the past, DOE management never provided the leadership commitment and resources necessary to address many of the problems, and the contractors who actually run the facilities were often recalcitrant. The labs, in particular, have been worlds unto themselves. The public and the media consider the lab employees, such as those at Los Alamos, to be DOE employees. They actually work for and are accountable to private contractors. For example, former DOE undersecretary Charles Curtis testified before the Senate Armed Services Committee recently that the labs refused to carry out his security directives. Security training for the scientists, who are the logical target for espionage, totaled 1-2 hours per year and focused on physical security.

The Subcommittee staff was just told yesterday of a deputy laboratory director who, when confronted by DOE with a computer security problem, said he was willing to take the risk of penetration of the system rather than improve security. The new lab director at Los Alamos is attempting to change that. Last fall, he initiated security "stand-down" days during which different offices take a day off to focus on security issues. He also has required senior lab management to participate in the security training which may be the first time these people have appeared at such a training. And a few weeks ago, Secretary Richardson shut down the computers and ordered the scientists to attend a week's worth of training.

This is a good start, but we still have questions about whether the site-specific security and safeguards plans are up to date. We wonder if the Department has an accurate overall threat assessment and site-specific vulnerability assessments so that it is spending its money in the right place.

The President says he would like $40 million for counter-intelligence at DOE. This is encouraging, but it also represents an enormous budget increase. We in Congress must make sure that this money can be used effectively. When the General Accounting Office tracked an earlier appropriation Congress made specifically for counter-intelligence, it found that most of it ended up in headquarters studies and excessive overhead charges by the individual facilities. Several reduced the amount of money they had allocated to counter-intelligence. The two labs implicated in the most recent allegations took the most in overhead. We don't want that to happen again. We need to take a close look at this request to make sure that we are fixing a problem, not just throwing money at it. Mr. Chairman, this Subcommittee has traditionally has had the endurance to review safeguards and security at these facilities after the press has moved on. I look forward to participating in the continuation of the oversight of the weapons facilities labs by the Subcommittee.

Mr. UPTON. Thank you, Mr. Klink.

A valuable member of this committee, though not a member of the subcommittee, is Heather Wilson, who, of course, represents parts of New Mexico. She has asked to sit in on the panel today, and with unanimous consent, I would like to ask that she might give an opening statement and participate as she can, following other members of this subcommittee, with questions and answers. Mrs. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman. I particularly appreciate your willingness to let me participate and observe in this process, as it is something that is very important to me, and very important to the country.

We should not be surprised that foreign governments have intelligence programs and intelligence collection programs targeted at our nuclear weapons facilities and our other military programs. The question is, whether we have adequate and effective counter-intelligence programs and security at our national laboratories, our military bases, and even at our higher headquarters, as far the Department of Defense, or as far as the National Security Council, and other places, where we might target intelligence efforts.

I think that we need to consider the information about national security and the national laboratories in context. That this is not about what exists at a point in time, whether that's 1988 or 1997, or today, but whether there is a system of security and counter-intelligence, over time and place, to constantly assess these things. It's not about the procedures today; it is about the system as a whole.

I believe that this committee, and as a country, we face two major challenges with respect to the review we are undertaking. First is to respond comprehensively, as a Nation, to meet the challenges posed by foreign governments who are trying to collect information about our military and nuclear weapons programs. The second is to avoid simplistic solutions that allow all of us to feel good, but which may not achieve the ends that we all want to achieve. And so we need to look at the substance. We need to avoid the tendency to wax rhetorical or give lip service, whether that is from the Department of Energy, the labs, those who testify before us today, or even Members of Congress. Let's get serious about this problem, and serious about the solutions.

It is easy to ask the questions and criticize, having before, served in a capacity where I sat at the desk responding to questions and criticisms; it is a lot harder to implement real change. So let's get down to what kinds of real changes need to be implemented. And

let us also make sure that we are focusing on the whole of the problem. In trying to explain what I mean by this, I was trying to think of how to illustrate this. My kids like to play with flashlights in the dark. And if you point the flashlights, you are focused on what is in the beam, and the scariest things are still in the dark. We would make a mistake if we focus on just what we see, or what we have paid attention to, in the past, and ignore the things that may still be in the dark. That is our challenge today.

Thank you, Mr. Chairman.

[Additional statements submitted for the record follow:]

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

We're here today to begin what I expect will be a series of hearings on the status of safeguards and security at the Department of Energy's nuclear weapon facilities, and in particular, its privately-run laboratories, which conduct this Nation's most highly sensitive, nuclear weapon-related research.

We've all heard a great deal recently about the very serious allegations of Chinese espionage at DOE's nuclear weapon labs. What we'll hear today is that none of these troubling events should have come as any surprise to us, given the long history of significant deficiencies in various aspects of DOE's security apparatus.

While a review of the written testimony for this hearing quickly reveals an incredible breadth of topics that can and should be explored, I must say that one particular area stands out in my mind—the fact that thousands of foreign scientists from countries such as China, Cuba, Iran, and Iraq are permitted to visit our most sensitive weapon laboratories and have fairly unrestricted exchanges with our scientists—including those working on matters that, while technically unclassified, are immensely useful to the weapon programs of foreign nations with potentially hostile intent towards the United States or its friends and allies around the world. China alone sent almost 1,500 scientists—including suspected intelligence agents—to our three most sensitive weapon labs during the time period 1994-1996 and, according to the testimony we've received today, less than two percent of those Chinese scientists received any background checks by the Department.

But my concern goes beyond the mere fact of whether the Department conducts an adequate background investigation on these foreign scientists. My concern goes to the very heart of this peculiar arrangement, and whether we are doing all that we should to give counter-intelligence training to those American scientists who must interact with foreign scientists, either here or abroad.

Our witnesses today are from the General Accounting Office and, collectively, they have spent decades critically analyzing DOE's security systems and recommending much-needed improvements along the way. I'm glad to have them here for this kick-off hearing on laboratory security, to give their perspective on some of the key factors underlying the general inability of the Department to get a firm and permanent handle on safeguards and security at its sensitive nuclear-weapon facilities.

Our purpose today is mostly educational—to help Members of Congress and the public put the current spy scandals in a broader, historical context. I should point out that the GAO currently is conducting, at this Committee's request, a comprehensive update of its key security work—and the work of other experts within and outside of the Department in this area—and will report back to us sometime later this year with a more current assessment of the Department's safeguards and security.

I also want to compliment the witnesses for getting their joint testimony to the Committee in a timely fashion—something that is, unfortunately, increasingly rare in my opinion. Timely written testimony really does help the Congress do its job, and makes these hearings much more useful and effective for both Members and the general public.

As I said at the start, I hope to continue this hearing in the not-too-distant future with other witnesses from the Department of Energy and its laboratories, so that we can more fully explore this important topic.

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

Thank you, Mr. Chairman, for holding this hearing. Security in our nation's nuclear laboratories is a subject that we should take very seriously. We should make

every effort to ensure that we are not contributing to the spread of technology that would allow the construction of nuclear weapons.

Mr. Chairman, we are here today to talk about the security problems that exist in some of our nation's foremost nuclear research laboratories. This is not a new problem; in fact, it has existed for many years.

Even though I have only served for three years on the Commerce Committee, it is my understanding that this Committee has done a great deal of work in the past 20 years to uncover and fix these problems.

I applaud the past work of this committee, and especially the ranking member, for that work and I hope that we can continue to work in a bipartisan fashion to improve the security that exists at these facilities.

However, Mr. Chairman, I do have some concerns about this hearing. While I understand the desire of the majority to establish a historical timeline and examine the conduct of the Department of Energy over that time period, I feel that the Department should have been represented at this hearing.

The Department of Energy deserves the opportunity to answer the testimony that we will be hearing from the GAO. I am disappointed that they will not receive that opportunity before this committee today.

Still, I look forward to hearing the comments of the GAO on the security arrangements, and I hope that this hearing will lead to the improvements that are necessary to increase the level of security in our nation's facilities.

Again, Mr. Chairman, thank you for holding this hearing.

PREPARED STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Thank you Mr. Chairman and thank you Ranking Member Klink. I'm glad to see the issue of DoE security is being addressed by this Subcommittee.

Just northwest of downtown Denver, Colorado is the former Department of Energy nuclear weapons facility Rocky Flats. Today this facility no longer produces weapons components, it has a new mission: environmental cleanup and closure. But part of that new mission includes managing the stockpile of nuclear materials that remained behind when weapons production was suspended in 1989. While recent attention has been given to safeguarding the technical "know-how" of weapons design, just as critical to the non-proliferation of nuclear weapons is the safeguarding and accounting of nuclear materials, such as the material at Rocky Flats. We also need assurance that Rocky Flats is protected against terrorism, domestic or international. While I recognize the nature of certain security precautions may be sensitive or classified, my constituents must be assured that Rocky Flats is beyond the reach of a Timothy McVeigh or an Osama bin-Laden. I look forward to hearing what GAO's findings have been regarding physical security at the Rocky Flats and other facilities.

I thank the GAO representatives for being here today to offer their perspective, and I thank the Subcommittee for addressing this important matter. I yield back the balance of my time.

Mr. UPTON. Thank you. To the witnesses and others, I want you to know that all of us on this subcommittee are on other subcommittees, and, in fact, there is a markup in the Health and Environment Subcommittee, of which I am also a member, and I hope that I do not get called to go downstairs. But that's where a number of our members are, and they will be coming back, hopefully, when that is over. But I would ask unanimous consent that all members of the subcommittee have a chance to put in an opening statement, and without objection, that will be so done.

We have a longstanding tradition, as you know, taking testimony under oath, and if all of you would rise and raise your right hand.

[Witnesses sworn.]

You are now sworn in. Generally the rule is that folks have testified for 5 minutes, but because of the sensitivity and the importance of this, and knowing that you are the only panel before us, we are going to waive that rule. All of your testimony will be made

part of the record, and we look forward to listening. The time is yours, Mr. Rezendes.

TESTIMONY OF VICTOR S. REZENDES, DIRECTOR, ENERGY, RESOURCES, AND SCIENCE ISSUES; ACCOMPANIED BY JOHN SCHULZE, ASSISTANT DIRECTOR, ENERGY, RESOURCES, AND SCIENCE ISSUES; WILLIAM FENZEL, ASSISTANT DIRECTOR, ENERGY, RESOURCES, AND SCIENCE ISSUES; AND GARY BOSS, ASSISTANT DIRECTOR, ENERGY, RESOURCES, AND SCIENCE ISSUES, GENERAL ACCOUNTING OFFICE

Mr. REZENDES. Thank you, Mr. Chairman. Over the past 20 years, we have performed numerous reviews of security that, unfortunately, Mr. Chairman, show serious weaknesses, that have led to loss of classified or sensitive information. While DOE has often agreed to take corrective action, implementation has often not been successful, and problems re-occur over the years. Let me highlight some of the problems. But first let me deal with foreign visitors.

In 1988, we reported that significant weaknesses exist in DOE controls over foreign visitors. Required background checks were performed for fewer than 10 percent of the visitors from sensitive countries. As a result, visitors with questionable backgrounds, including connections with foreign intelligence services, obtained access to laboratories without DOE's knowledge. Those in the laboratories were not always aware of those topics that DOE considered sensitive. Visits were occurring without authorized approvals; security plans detailing how the visits would be controlled were not prepared, and DOE was not notified of all the visits. Although DOE agreed to take corrective action, we found that at the same time the number of visitors continued to grow. The annual number of foreign visitors increased nearly 70 percent, to about 6,400 per year. Those from sensitive countries increased 250 percent.

We again examined controls over foreign visitors 9 years later, and found that the problems persisted. The revised procedures for obtaining background checks had not been effectively implemented at two facilities. Fewer background checks were being conducted with only 5 percent of the visitors from sensitive countries, and less than 2 percent of those from China, receiving background checks. We also found that visits were still occurring that involved many sensitive topics, without DOE's knowledge. Security controls over foreign visitors did not preclude them from obtaining access to sensitive information. Los Alamos allowed unescorted, after-hours access to controlled areas to preserve, as one official called it, "an open campus atmosphere." Additionally, we found that counterintelligence programs lacked key data on the threats to the facility, and how well the facilities were protected from those threats.

Let me switch now to information security. This area involved protecting classified information from inappropriate disclosure. In the early 1990's, we found problems that could involve a loss of classified information. Lawrence Livermore, a national laboratory, was unable to locate 10,000 secret documents. Although the laboratory's controls were evaluated annually, the evaluations were limited in scope, and failed to identify the documents we were missing.

In prior years, we reported that DOE had internal controls over unclassified, but still sensitive information that could assist foreign

nuclear weapons programs. Specifically, we found countries like, China, India, Iraq, Pakistan, routinely obtained re-processing and nuclear weapons related information directly from the Department of Information. As recently as February of this year, we reported on information security problems in DOE's initiative for proliferation prevention with Russia. Under this initiative, DOE has provided defense-related information to Russian weapon scientists. We reviewed 79 of these projects—they were funded under DOE's programs—and found 9 to be dual-use projects.

Another security weakness that is involved is physical security controls; in essence, this is the guns, guards, and gates at DOE facilities. In the 1990's we reported that security personnel were unable to demonstrate basic skills, such as handcuffing, searching, and arresting intruders, as well as shooting accurately. We found at Los Alamos 78 percent of the security force failed to pass required skill tests.

The problems we identified were not only with keeping threats out of the facility, but also with keeping property in. For example, we reported that Lawrence Livermore could not locate 16 percent of its inventory of government property. When we returned a year later to re-visit this problem, we found that only 3 percent of the missing property had been found. Moreover, the laboratory's accounting controls for this equipment were weaker than they were in the previous year.

The next area involves personnel security issues, which is intended to provide assurance that personnel with access to classified information, are trustworthy. We found numerous problems in this area, dating back to the 1980's. Clearance files at two offices contained over 4,000 clearances that should have been terminated, and over 600 employees at Los Alamos had clearance badges, but did not have active clearances in their files. In addition, some DOE contractors were not verifying information on prospective employees, such as credit and law enforcement records.

The last area of concern related to material accountability, which concerns the protection of special nuclear materials, such as enriched uranium and plutonium. In 1991, we found that DOE facilities were not properly measuring, storing, and verifying quantities of nuclear materials. Without proper accounting for this material, missing quantities are difficult to detect. Over the years, DOE has been unable to account for substantial amounts of enriched uranium and plutonium.

We also reported on DOE's efforts to develop a nuclear tracking system for monitoring nuclear materials exported to foreign countries. We reported that the existing system was not able to track all exported nuclear materials. Moreover, DOE had not adequately planned a replacement system. Our concerns were well justified. Within 3 months after the new tracking system began operating, the technical committee overseeing this system concluded that the system faced a high probability of failure, and the system should not be used.

As you can see, Mr. Chairman, our work over the years has identified a wide variety of specific security problems at DOE's facilities. While each individual security problem is a concern, when

looked at collectively over an extended period of time, a more serious situation becomes apparent, that stems from systemic causes.

First, there has been a longstanding lack of attention and priority given to security matters by DOE managers, and their contractors. For example, in 1988, in response to our foreign visitors report, DOE brought in FBI personnel to assist its the counterintelligence program. However, the FBI eventually withdrew its personnel, because of resistance within DOE to implement any of the measures the FBI staff believed were necessary to improve security. We know that, in response to the current concerns, the FBI is again being brought into DOE to head up the counterintelligence program.

As far back as 1980, we reported that funding for security had low priority and little visibility. In 1992, we reported that safeguard and security plans, and vulnerability assessments for many of DOE's most sensitive facilities were almost 2 years overdue because, in part, DOE had not provided sufficient staff to get the job done. Similarly, security problems identified by DOE's own internal security staff often go unresolved, even today.

For example, issues relating to inadequate separation between classified and unclassified computer networks were identified in Los Alamos in 1988, in 1992, and again in 1994. This problem was discovered again at Los Alamos just last year. The Secretary of Energy ordered a shutdown of classified computers at these, the three defense laboratories, and directed the staff to attend computer security training.

We reported, in 1997, that DOE had not developed measures for evaluating counterintelligence at its laboratories. The low priority given security matters is underscored in how DOE manages its contract with the University of California, both at Los Alamos and Livermore. Performance measures for counterintelligence activities are still not in its contracts with these two laboratories. We recommended, as far back as 1990, that DOE should withhold a contractor's fee for failing to fix security problems on a timely basis. DOE just recently announced a new policy which would allow it to do just that.

In the final analysis, security problems reflect a lack of accountability. Security problems have languished for years without resolution or repercussion to those responsible. The well-documented history of security lapses shows that DOE is not holding its contractors accountable, and DOE leadership is not holding its program managers accountable for making sure contractors do their job. Achieving accountability in DOE is made more difficult by its complex organizational structure. The FBI, which examined DOE's counterintelligence activities, noted that there is a gap between authority and responsibility, particularly when national interests compete with the specialized interest of the academic or corporate management that operates the laboratories. Citing the laboratories autonomy, granted by DOE, the FBI found that this autonomy made national guidance, oversight, and accountability of the laboratories' counterintelligence programs arduous and inefficient. Other groups have also reported accountability problems at DOE from unclear lines of command.

We believe these organizational weaknesses are a major reason why DOE has been unable to develop long-term solutions to re-occurring problems. Continued vigilance, as well as more sophisticated security strategies, will be needed to meet the threats that exist today. Mr. Chairman, we are concerned that, given DOE's past track record, they may not be up to the challenge without congressional oversight to hold them accountable for achieving specific goals, and for objectives in security reform. Thank you.

[The prepared statement of Victor S. Rezendes follows:]

PREPARED STATEMENT OF VICTOR S. REZENDES, DIRECTOR, ENERGY, RESOURCES AND SCIENCE ISSUES, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION, UNITED STATES GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee: We are pleased to be here today to discuss our past work involving security at the Department of Energy's (DOE) facilities. These facilities, particularly its nuclear weapons design laboratories and its nuclear material and weapons production facilities, have long been viewed by DOE and the FBI as targets of espionage and other threats. Recent revelations of the possible loss of nuclear weapons design and other classified information to foreign countries have focused renewed attention on the effectiveness of security at DOE's facilities and have prompted concerns at high levels in the government, including the Administration and the Congress.

To protect its facilities from security threats, DOE created a multifaceted, defense-in-depth security strategy. Under such a strategy, various lines of defense are used to protect classified and sensitive information, nuclear materials, and equipment. Over the last 20 years, we have performed numerous reviews of security that, unfortunately, Mr. Chairman, show serious weaknesses in many of these lines of defense that have lead to losses of classified or sensitive information and technology.

In summary, Mr. Chairman, our work has identified security-related problems with controlling foreign visitors, protecting classified and sensitive information, maintaining physical security over facilities and property, ensuring the trustworthiness of employees, and accounting for nuclear materials. These problems include:

- Ineffective controls over foreign visitors to DOE's most sensitive facilities. We found in 1988, and again in 1997, that foreign visitors are allowed into DOE's nuclear weapons design laboratories with few background checks and inadequate controls over the topics discussed, and that other security procedures, such as access controls, to mitigate the risks from these visits may not be fully effective. In addition, counterintelligence programs to guard against foreign and industrial espionage activities received little priority and attention.
- Weaknesses in efforts to control and protect classified and sensitive information. We found one instance where a facility could not account for 10,000 classified documents. In 1987, 1989, and 1991, we reported that foreign countries routinely obtained unclassified but sensitive information that could assist their nuclear weapons capability. Earlier this year, we reported that under its program with Russia to prevent proliferation, DOE may have provided Russian scientists with dual-use defense-related information that could negatively affect national security.
- Lax physical security controls, such as security personnel and fences, to protect facilities and property. Our reviews of security personnel have shown that these personnel have been unable to demonstrate basic skills such as arresting intruders or shooting accurately; at one facility, 78 percent of the security personnel failed a test of required skills. Furthermore, we found that equipment and property worth millions of dollars was missing at some facilities.
- Ineffective management of personnel security clearance programs has been a problem since the early 1980s. Backlogs were occurring in conducting security investigations, and later when the backlogs were reduced, we found some contractors were not verifying information on prospective employees.
- Weaknesses in DOE's ability to track and control nuclear materials. We reported in 1980 and again in 1991 that, at some facilities, DOE was not properly, measuring, storing, and verifying quantities of nuclear materials. Also, DOE was not able to track all nuclear material sent overseas for research and other purposes.

The recent revelations about espionage bring to light how ingrained security problems are at DOE. Although each individual security problem is a concern, when these problems are looked at collectively over time, a more serious situation becomes

apparent. While a number of investigations are currently underway to determine the status of these security problems, we have found that DOE has often agreed to take corrective action but the implementation has not been successful and the problems reoccur. In our view, there are two overall systemic causes for this situation. First, DOE managers and contractors have shown a lack of attention and/or priority to security matters. Second, and probably most importantly, there is a serious lack of accountability at DOE. Efforts to address security problems have languished for years without resolution or repercussions to those organizations responsible.

Security in today's environment is even more challenging, given the greater openness that now exists at DOE's facilities and the international cooperation associated with some of DOE's research. Even when more stringent security measures were in place than there are today, such as those in effect during the development of the first atomic bombs, problems have arisen and secrets can be, and were, lost. Consequently, continual vigilance, as well as more sophisticated security strategies, will be needed to meet the threats that exist today. Mr. Chairman, we are concerned that, given DOE's past record, it may not be up to the challenge without congressional oversight to hold it accountable for achieving specific goals and objectives for security reform. Therefore, we are pleased that the Committee has taken a special interest in DOE's security problems and we have already begun to work on the Committee's request to have us assess the current status of these security problems.

BACKGROUND

DOE has numerous contractor-operated facilities that carry out the programs and missions of the Department. Much of the work conducted at these facilities is unclassified and nonsensitive and can be, and is, openly discussed and shared with researchers and others throughout the world. However, DOE's facilities also conduct some of the nation's most sensitive activities, including designing, producing, and maintaining the nation's nuclear weapons; conducting efforts for other military or national security applications; and performing research and development in advanced technologies for potential defense and commercial applications.

Security concerns and problems have existed since these facilities were created. The Los Alamos National Laboratory in New Mexico developed the first nuclear weapons during the Manhattan Project in the 1940s; however, it was also the target of espionage during that decade as the then Soviet Union obtained key nuclear weapons information from the laboratory. In the 1960s, significant amounts of highly enriched uranium—a key nuclear weapons material—was discovered to be missing from a private facility under the jurisdiction of the Atomic Energy Commission, a predecessor to DOE. It is widely believed that in the early 1980s, China obtained information on neutron bomb design from the Lawrence Livermore National Laboratory in California.

Most recently, two incidents have occurred at Los Alamos in which laboratory employees are believed to have provided classified information to China. In one situation, a laboratory employee admitted to providing China classified information on a technology used to conduct nuclear weapons development and testing. In the other situation, which occurred earlier this year, DOE disclosed that it had evidence that indicated China obtained information on this nation's most advanced nuclear warhead and had used that information to develop its own smaller, more deliverable nuclear weapons. A laboratory employee has been fired as a result of recent investigations into how this information was obtained by China; however, no charges have yet been filled.

PROBLEMS NOTED IN CRITICAL SECURITY AREAS

While the recent incidents at Los Alamos have been receiving national attention, these are only the most recent examples of problems with DOE's security systems. For nearly 20 years, we have issued numerous reports on a wide range of DOE security programs designed to protect nuclear weapons-related and other sensitive information and material. These reports have included nearly 50 recommendations for improving programs for controlling foreign visitor access, protecting classified and sensitive information, maintaining physical security over facilities and property, ensuring the trustworthiness of employees, and accounting for nuclear materials. While DOE has often agreed to take corrective actions, we have found that the implementation has often not been successful and that problems recur over the years. I would like to highlight some of the security problems identified in these reports.

Inadeguate Controls Over Foreign Visitors

Thousands of foreign nationals visit DOE facilities each year, including the three laboratories—Lawrence Livermore National Laboratory in California and the Los

Alamos National Laboratory and the Sandia National Laboratories in New Mexico[1]—that are responsible for designing and maintaining the nation's nuclear weapons. These visits occur to stimulate the exchange of ideas, promote cooperation, and enhance research efforts in unclassified areas and subjects. However, allowing foreign nationals into the weapons laboratories is not without risk, as this allows foreign nationals direct and possibly long-term access to employees with knowledge of nuclear weapons and other sensitive information. Consequently, DOE has had procedures to control these visits as well as other lines of defense—such as access controls and counterintelligence programs—to protect its information and technology from loss to foreign visitors.

In 1988, we reported that significant weaknesses exist in DOE's controls over foreign visitors to these laboratories.[2] First, required background checks were performed for fewer than 10 percent of the visitors from sensitive countries prior to their visit.[3] As a result, visitors with questionable backgrounds—including connections with foreign intelligence services—obtained access to the laboratories without DOE's knowledge. Second, DOE and the laboratories were not always aware of visits that involved topics, such as isotope separation and inertial confinement fusion, that DOE considers sensitive because they have the potential to enhance nuclear weapons capability, lead to proliferation, or reveal other advanced technologies. Third, internal controls over the foreign visitor program were ineffective. Visits were occurring without authorized approvals, security plans detailing how the visits would be controlled were not prepared, and DOE was not notified of visits. Because DOE was not notified of the visits, it was unaware of the extent of foreign visitors to the laboratories.

At that time, DOE acknowledged problems with its controls over foreign visitors and subsequently set out to resolve these problems. Among other things, DOE revised its foreign visitor controls, expanded background check requirements, established an Office of Counterintelligence at DOE headquarters, and created an integrated computer network for obtaining and disseminating data on foreign visitors. However, at the same time the number of foreign visitors continued to grow. Between the period of the late-1980s to the mid-1990s, the annual number of foreign visitors increased from about 3,800 to 6,400 per year—nearly 70 percent—and those from sensitive countries increased from about 500 to over 1,800 per year—more than 250 percent.

We again examined the controls over foreign visitors and reported in 1997 that most of the problems with these controls persist.[4] We found that revised procedures for obtaining background checks had not been effectively implemented and that at two facilities, background checks were being conducted on only 5 percent of visitors from all sensitive countries and on less than 2 percent of the visitors from China. We also found that visits were still occurring that may involve sensitive topics without DOE's knowledge. Moreover, other lines of defense were not working effectively. Security controls over foreign visitors did not preclude them from obtaining access to sensitive information. For example, Los Alamos allowed unescorted after-hours access to controlled areas to preserve what one official described as an open "campus atmosphere." Evaluations of the controls in areas most frequented by foreign visitors had not been conducted.

Additionally, we found that the counterintelligence programs for mitigating the threat posed by foreign visitors needed improvements. These programs lacked comprehensive threat assessments, which are needed to identify the threats against DOE and the facilities most at risk, and lacked performance measures to gauge the effectiveness of these programs in neutralizing or deterring foreign espionage efforts. Without these tools, the counterintelligence programs lacked key data on threats to the facilities and on how well the facilities were protected against these threats.

Information Security

Information security involves protecting classified and/or sensitive information from inappropriate disclosure. We have found problems with information security at the nuclear weapons laboratories that could involve the loss of classified information and/or assist foreign nuclear weapons capability. For example, in February 1991, we

---

[1] Sandia also has a facility adjacent to the Lawrence Livermore facility in California.

[2] *Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories* (GAO/RCED-89-31, Oct. 11, 1988).

[3] DOE's definition of sensitive countries has changed over time. Currently, DOE views certain countries as sensitive because of concerns about national security, nuclear nonproliferation, regional instability, or support of terrorism.

[4] *Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories* (GAO/RCED-97-229, Sept. 25, 1997).

reported that the Lawrence Livermore National Laboratory was unable to locate or determine the disposition of over 12,000 secret documents.[5] These documents covered a wide range of topics, including nuclear weapons design. The laboratory conducted a search and located about 2,000 of these documents but did not conduct an assessment of the potential that the documents still missing compromised national security. We also found that DOE had not provided adequate oversight of the laboratory's classified document control program. Although the laboratory's classified document controls were evaluated annually, the evaluations were limited in scope and failed to identify that documents were missing.

In 1987 and 1989, we reported that DOE had inadequate controls over unclassified but sensitive information that could assist foreign nuclear weapons programs.[6] Specifically, we found that countries—such as China, India, Iraq, and Paldstan—that pose a proliferation or security risk routinely obtain reprocessing and nuclear weapon-related information from DOE. We also found that DOE had transferred to other countries information appearing to meet the definition of sensitive nuclear technology, which requires export controls. Further, we found that DOE placed no restrictions on foreign nationals' involvement in reprocessing research at colleges and universities.

In the 1990s, we continued to raise concerns. In 1991, we reported that DOE and its weapons laboratories were not complying with regulations designed to control the risk of weapons technology or material being transferred to foreign countries having ownership, control, or influence over U.S. companies performing classified work for DOE.[7] We estimated that about 98 percent of the classified contracts awarded at the weapons laboratories during a 30-month period that were subject to such regulations did not fully comply with those regulations.

As recently as February of this year, we reported on information security problems in DOE's Initiatives for Proliferation Prevention with Russia.[8] Under these initiatives, DOE may have provided defense-related information to Russian weapons scientists—an activity that could negatively affect U.S. national security. We reviewed 79 projects funded by DOE under this program and found nine to have dual-use implications—that is, both military and civilian applications—such as improving aircraft protective coating materials, enhancing communication capabilities among Russia's closed nuclear cities, and improving metals that could be used in military aircraft engines.

We note that the Department of Commerce has also recently raised concerns about nuclear-related exports to Russia from at least one DOE facility. Commerce notified Los Alamos in January 1999 that equipment the laboratory sent to nuclear facilities in Russia required export licenses and that the laboratory may be facing civil charges for not obtaining the required licenses.

Physical Security

Physical security controls involve the protection, primarily through security personnel and fences, of facilities and property. In 1991, we reported that security personnel were unable to demonstrate basic skills such as the apprehension and arrest of individuals who could represent a security threat.[9] Prior to that report, in 1990, we reported that weaknesses were occurring with security personnel, as some security personnel could not appropriately handcuff, search, or arrest intruders or shoot accurately.[10] For example, we found that at the Los Alamos National Laboratory, 78 percent of the security personnel failed a test of required skills. Of the 54-member guard force, 42 failed to demonstrate adequate skill in using weapons, using a baton, or apprehending a person threatening the facility's security. Some failed more than one skill test. We also found that many Los Alamos' training records for security personnel were missing, incomplete, undated, changed, or unsigned. With-

---

[5] *Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate* (GAO/RCED-91-65, Feb. 8, 1991).

[6] *Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information* (GAO/RCED-87-150, Aug. 17, 1987) and *Nuclear Nonproliferation: Better Controls Needed Over Weapons-Related Technology* (GAO/RCED-89-116, Jun. 19, 1989).

[7] *Nuclear Nonproliferation: DOE Needs Better Controls to Identify Having Foreign Interests* (GAO/RCED-91-83, Mar. 25, 1991).

[8] *Nuclear Nonproliferation: Concerns With DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists* (GAO/RCED-99-54, Feb. 19, 1999).

[9] *Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities* (GAO/RCED-92-39, Dec. 13, 1991).

[10] *Nuclear Safety: Potential Security Weaknesses at Los Alamos and other DOE Facilities* (GAO/RCED-91-12, Oct. 11, 1990).

out accurate and complete training records, DOE could not demonstrate that security personnel are properly trained to protect the facility.

Problems we have identified were not only with keeping threats out of the facilities, but also with keeping property in. For example, we reported in 1990 that the Lawrence Livermore National Laboratory could not locate about 16 percent of its inventory of government equipment, including video and photographic equipment as well as computers and computer-related equipment.[11] When we returned in 1991 to revisit this problem, we found that only about 3 percent of the missing equipment had been found; moreover, the laboratory's accountability controls over the equipment were weaker than in the prior year.[12] We also found that DOE's oversight of the situation was inadequate and that its property control policies were incomplete. We found similar problems at DOE's Rocky Flats Plant in 1994 where property worth millions of dollars was missing, such as forklift and a semi-trailer. Eventually, property worth almost $21 million was written off.[13]

Other problems in controlling sensitive equipment have been identified, such as disposing of usable nuclear-related equipment, that could pose a proliferation risk. For example, in 1993, DOE sold 57 different components of nuclear fuel reprocessing equipment and associated design documents, including blueprints, to an Idaho salvage dealer. DOE subsequently determined that the equipment and documents could be useful to a group or country with nuclear material to process, and that the equipment could significantly shorten the time necessary to develop and implement a nuclear materials reprocessing operation. This incident resulted from a lack of vigilance at all levels for the potential impacts of releasing sensitive equipment and information to the public, and DOE conceded that system breakdowns of this type could have severe consequences in other similar situations where the equipment and documents may be extremely sensitive.

Personnel Security

DOE's personnel security clearance program is intended to provide assurance that personnel with access to classified material and information are trustworthy. We have found numerous problems in this area, dating back to the early 1980s. In 1987, and again in 1988, we found that DOE headquarters and some field offices were taking too long to conduct security investigations.[14] We found that the delays in investigations lowered productivity, increased costs, and were a security concern. We also found that DOE's security clearance database was inaccurate. Clearance files at two field offices contained about 4,600 clearances that should have been terminated and over 600 employees at the Los Alamos laboratory had clearance badges, but did not have active clearances listed in the files. In other cases, the files contained inaccurate data, such as incorrect clearance levels and names. We followed DOE's efforts to remedy these problems, and by 1993, DOE had greatly reduced its backlog of investigations.[15] However, some DOE contractors were not verifying information on prospective employees such as education, personal references, previous employment, and credit and law enforcement records.

Accounting for Nuclear Material

Material accountability relates to the protection of special nuclear material such as enriched uranium and plutonium. In 1991, we found that DOE facilities were not properly measuring, storing, and verifying quantities of nuclear materials.[16] Without proper accounting for nuclear materials, missing quantities are more difficult to detect. We also found that DOE facilities were not complying with a rule requiring that two people always be present when nuclear material is being accessed or used. This rule is designed to preclude a single individual from having access to and diverting nuclear material without detection.

---

[11] *Nuclear Security: DOE Oversight of Livermore's Property Management System Is Inadequate* (GAO/RCED-90-122, Apr. 18, 1990).

[12] *Nuclear Security: Property Control Problems at DOE's Livermore Laboratory Continue* (GAO/RCED-91-141, May 16, 1991).

[13] *Department of Energy: The Property Management System at the Rocky Flats Plant Is Inadeguate* (GAO/RCED-94-77, Mar. 1, 1994).

[14] *Nuclear Security: DOE's Reinvestigation of Employees Has Not Been Timely* (GAO/RCED-87-72, Mar. 10, 1987) and *Nuclear Security: DOE, Needs a More Accurate and Efficient Security Clearance Program* (GAO/RCED-88-28, Dec. 29, 1987).

[15] *Nuclear Security: DOE's Progress on Reducing Its Security Clearance Work Load* (GAO/RCED-93-183, Aug. 12, 1993).

[16] *Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities* (GAO/RCED-92-39, Dec. 13, 1991).

In 1994 and 1995, we reported on DOE's efforts to develop a nuclear material trading system for monitoring nuclear materials exported to foreign countries.[17] A nuclear tracking system is important to protect nuclear materials from loss, theft, or diversion. In 1994, we reported that the existing system was not able to track all exported nuclear materials and equipment; moreover, DOE had not adequately planned the replacement system. We recommended activities that we believed were necessary to ensure that the new system would be successful. In 1995, we found that DOE had not implemented our recommendations and had no plans to do so. We also found that the system still had development risks. DOE was not adequately addressing these risks and had no plans to conduct acceptance testing, and as a result of these problems, it had no assurance that the system would ever perform as intended. Our concerns were justified, as 3 months after the new tracking system began operating, the technical committee overseeing this system concluded that it faced a high probability of failure and that the system should not be used.

KEY FACTORS CONTRIBUTING TO SECURITY PROBLEMS

As you can see, Mr. Chairman, our work over the years has identified a wide variety of specific security problems at DOE facilities. While each individual security problem is a concern, when looked at collectively over an extended period of time, a more serious situation becomes apparent that stems from systemic causes. In our view, there are two overall systemic causes of the security problems. First, there has been a longstanding lack of attention and/or priority given to security matters by DOE managers and its contractors. Second, and probably most importantly, there is a serious lack of accountability among DOE and its contractors for their actions. These two causes are interrelated and not easily corrected.

Lack of Attention and Priority to Security

The lack of attention and priority given by DOE management and its contractors to security matters can be seen in many areas. One area is its long-term commitment to improving security. For example, in response to our 1988 report on foreign visitors, DOE required more background checks be obtained. However, 6 years later, it granted Los Alamos and Sandia exemptions to this requirement, and as a result, few background checks were conducted at those facilities. Also in response to our 1988 report, DOE brought in FBI personnel to assist its counterintelligence programs. However, the FBI eventually withdrew its personnel in the early 1990s because of resistance within DOE to implementing the measures the FBI staff believed necessary to improve security. We note with interest that in response to the current concerns with foreign visitors and other espionage threats against DOE facilities, the FBI is again being brought in to direct DOE's counterintelligence program.

The lack of attention to security matters can be seen in other ways as well. In 1996, when foreign visitors were coming in increasing numbers to the laboratory, Los Alamos funded only 1.1 staff years for its counterintelligence program. Essentially, one person had to monitor not only thousands of visitors to the laboratory but also monitor over 1,000 visits made by laboratory scientists overseas. This problem was not isolated to Los Alamos; funding for counterintelligence activities at DOE facilities during the mid-1990s could only be considered minimal. Prior to fiscal year 1997, DOE provided no direct funding for counterintelligence programs at its facilities. Consequently, at eight high-risk facilities, counterintelligence program funding was obtained from overhead accounts and totaled only $1.4 million and 15 staff. Resources were inadequate in other areas. In 1992, we reported that safeguard and security plans and vulnerability assessments for many of DOE's sensitive facilities were almost 2 years overdue because, among other reasons, DOE had not provided sufficient staff to get the job done. These plans and assessments are important in identifying threats to the facilities as well as devising countermeasures to the threats. In our view, not providing sufficient resources to these important activities indicates that security is not a top priority. This problem is not new. We reported in 1980 and again in 1982 that funding for security has low priority and little visibility.[18]

---

[17] *Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking Capabilities Are Limited* (GAO/RCED/AIMD-95-5, Dec. 27, 1994) and *Department of Energy: Poor Management of Nuclear Materials Tracking System Makes Success Unlikely* (GAO/AIMD—95-165, Aug. 3, 1995).

[18] *Nuclear Fuel Reprocessing and the Problems of Safeguarding Against the Spread of Nuclear Weapons* (EMD-80-38, Mar. 18, 1980) and *Safeguards and Security At DOE's Weapons Facilities Are Still Not Adequate,* (C-GAO/EMD-82-1, Aug. 20, 1982).

Earlier I mentioned missing classified documents at Lawrence Livermore Laboratory. In response to that report, both DOE and laboratory officials showed little concern for the seriousness of the situation and told us that they believed the missing documents were the result of administrative error, such as inaccurate record keeping and not theft. Although DOE is required to conduct an assessment of the missing documents' potential for compromising national security, at the time of our report DOE did not plan to do this for over 1 year after we reported the documents missing.

Similarly, security problems identified by DOE's own internal security oversight staff often go unresolved, even today. For example, issues related to the inadequate separation of classified and unclassified computer networks were identified at Los Alamos in 1988, 1992, and 1994. This problem was only partially corrected in 1997, as classified information was discovered on Los Alamos' unclassified computer network in 1998. We found in 1991 that deficiencies DOE identified as early as 1985 at six facilities had not been corrected by 1990 because DOE did not have a systematic method to track corrective actions taken on its own security inspections.

The low priority given security matters is underscored by how DOE manages its contractors. DOE's contract with the University of California for managing its Los Alamos and Lawrence Livermore national laboratories contain specific measures for evaluating the university's performance. These measures are reviewed annually by DOE and should reflect the most important activities of the contractor. However, none of the 102 measures in the Los Alamos contract or the 86 measures in the Lawrence Livermore contract relate to counterintelligence. We reported in 1997 that DOE had not developed measures for evaluating the laboratories' counterintelligence activities, and DOE told us it was considering amending its contracts to address this problem. Performance measures for counterintelligence activities are still not in its contracts for these two laboratories. The contracts do contain a related measure, for safeguarding classified documents and materials from unauthorized persons, but this measure represents less than 1 percent of the contractor's total score. Safeguards and security performance measures in general account for only about 5 percent of the university's performance evaluations for the two laboratories.

The low priority afforded security matters may account for the low rating DOE has just given nuclear weapons facilities in its latest Annual Report on Safeguards and Security. Two weapons laboratories—Los Alamos and Lawrence Livermore—received a rating of "marginal" for 1997 and 1998. In its annual evaluation of Los Alamos' overall performance, however, DOE rated the laboratory as "excellent" in safeguards and security, even though the laboratory reported 45 classified matter compromises and infractions for the year. The previous 3-year rolling average was 20. DOE explained that the overall excellent score was justified based on Los Alamos' performance in many different aspects of safeguards and security. For future contracts, a new DOE policy will enable the Department to withhold a laboratory's full fee for catastrophic events, such as a loss of control over classified material. We recommended as far back as 1990 that DOE should withhold a contractor's fee for failing to fix security problems on a timely basis. Both laboratories have been managed by the University of California since their inception without recompeting these contracts, making them among the longest-running contracts in the DOE complex.

Lack of Accountability

In the final analysis, security problems reflect a lack of accountability. The well-documented history of security lapses in the nuclear weapons complex show that DOE is not holding its contractors accountable for meeting all of its important responsibilities. Furthermore, DOE leadership is not holding its program managers accountable for making sure contractors do their jobs.

Achieving accountability in DOE is made more difficult by its complex organizational structure. Past advisory groups and internal DOE studies have often reported on DOE's complex organizational structure and the problems in accountability that result from unclear chains of command among headquarters, field offices, and contractors. For example

- The FBI, which examined DOE's counterintelligence activities in 1997, noted that there is a gap between authority and responsibility, particularly when national interests compete with specialized interests of the academic or corporate management that operate the laboratories. Citing the laboratories' autonomy granted by DOE, the FBI found that this autonomy has made national guidance, oversight, and accountability of the laboratories' counterintelligence programs arduous and inefficient.
- A 1997 report by the Institute for Defense Analyses cited serious flaws in DOE's organizational structure. Noting long-standing concerns in DOE about how best to define the relationships between field offices and the headquarters program

offices that sponsor work, the Institute concluded that "the overall picture that emerges is one of considerable confusion over vertical relationships and the roles of line and staff officials." As a consequence of DOE's complex structure, the Institute reported that unclear chains of command led to the weak integration of programs and functions across the Department, and confusion over the difference between line and staff roles.[19]

- A 1997 DOE internal report stated that "lack of clarity, inconsistency, and variability in the relationship between headquarters management and field organizations has been a longstanding criticism of DOE operations . . . This is particularly true in situations when several headquarters programs fund activities at laboratories . . ." [20]
- DOE's Laboratory Operations Board also reported in 1997 on DOE's organizational problems, noting that there were inefficiencies due to DOE's complicated management structure. The Board recommended that DOE undertake a major effort to rationalize and simplify its headquarters and field management structure to clarify roles and responsibilities.[21]

DOE's complex organization stems from the multiple levels of reporting that exist between contractors, field offices, and headquarters program offices. Further complicating reporting, DOE assigns each laboratory to a field operations office, whose director serves as the contract manager and also prepares the contractor's annual appraisal. The operations office, however, reports to a separate headquarters office under the Deputy Secretary, not to the program office that supplies the funding. Thus, while the Los Alamos National Laboratory is primarily funded by Defense Programs, it reports to a field manager who reports to another part of the agency.

We believe these organizational weaknesses are a major reason why DOE has been unable to develop long-term solutions to the recurring problems reported by advisory groups. Recent events at the Brookhaven National Laboratory in New York, for example, illustrate the consequences of organizational confusion. Former Secretary Peña fired the contractor operating the laboratory when he learned that the contractor breached the community's trust by failing to ensure it could operate safely. DOE did not have a clear chain of command over environment, safety, and health matters and, as a result, laboratory performance suffered in the absence of DOE accountability. To address problems in DOE's oversight, the Secretary removed the Chicago Operations Office from the chain of command over Brookhaven, by having the on-site DOE staff report directly to the Secretary's office. We found, however, that even though the on-site staff was technically reporting directly to the Secretary's office, the Chicago Operations Office was still managing the contractor on a day-today basis, including retaining the responsibility for preparing the laboratory's annual appraisal. Chicago officials told us that there was considerable confusion regarding the roles of Chicago and on-site DOE staff. As a result, DOE did not fundamentally change how it manages the contractor through its field offices.

This concludes my testimony, and I will be happy to answer any questions you may have.

Appendix

Nuclear Fuel Reprocessing And The Problems Of Safeguarding Against The Spread Of Nuclear Weapons, (EMD-80-38, Mar. 18, 1980).

Nuclear Fuel Reprocessing and the Problems of Safeguarding Against the Spread of Nuclear Weapons (EMD-80-38, Mar. 18, 1980).

Safeguards and Securely At DOE's Weapons Facilities Are Still Not Adequate (C-GAO/EMD-82-1, Aug. 20, 1982).

Security Concerns at DOE's Rocky Flats Nuclear Weapons Production Facility (GAO/RCED—85-83).

Nuclear Nonproliferation: DOE Has Insufficient Control Over Nuclear Technology Exports (GAO/RCED-86-144, May 1, 1986).

Nuclear Security: DOE's Reinvestigation of Employees Has Not Been Timely (GAO/RCED-87-72, Mar. 10, 1987).

Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information (GAO/RCED-87-150, Aug. 17, 1987).

Nuclear Security: DOE Needs a More Accurate and Efficient Security Clearance Program (GAO/RCED-88-28, Dec. 29, 1987).

Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31, Oct. 11, 1988).

---

[19] *The Organization and management of the Nuclear Weapons Program, Institute for Defense Analyses* (March 1997).

[20] *DOE Action Plan for Improved Management of Brookhaven National Laboratory,* DOE (July 1997).

[21] *Department of Energy: Uncertain Progress in Implementing National Laboratory Reforms*, (GAO/RCED-98-197, Sept. 10, 1998).

Nuclear Security: DOE Actions to Improve the Personnel Clearance Program (GAO/RCED-89-34, Nov. 9, 1988).
Nuclear Nonproliferation: Better Controls Needed Over Weapons-Related Information and Technology (GAO/RCED-89-116, Jun. 19, 1989).
Nuclear Security: DOE Oversight Livermore's Property Management System Is Inadequate (GAO/RCED-90-122, Apr. 18, 1990).
Nuclear Safely: Potential Security Weaknesses At Los Alamos and Other DOE Facilities (GAO/RCED-91-12, Oct. 11, 1990).
Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate (GAO/RCED-91-65, Feb. 8, 1991).
Nuclear Nonproliferation: DOE Needs Better Controls to Identify Contractors Having Foreign Interests (GAO/RCED-91-83, Mar. 25, 1991).
Nuclear Security: Property Control Problems at DOE's Livermore Laboratory Continue (GAO/RCED-91-141, May 16.1991).
Nuclear Security: DOE Original Classification Authority Has Been Improperly Delegated (GAO/RCED-91-183, July 5, 1991).
Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities (GAO/RCED-92-39, Dec. 13, 1991).
Nuclear Security: Weak Internal Controls Hamper Oversight of DOE's Security Program (GAO/RCED-92-146, June 29, 1992).
Nuclear Security: Improving Correction of Security Deficiencies at DOE's Weapons Facilities (GAO/RCED-93-10, Nov. 16, 1992).
Nuclear Security: Safeguards and Security Planning at DOE Facilities Incomplete (GAO/RCED-93-14, Oct. 30, 1992).
Personnel Security: Efforts by DOD and DOE to Eliminate Duplicative Background Investigations (GAO/RCED-93-23, May 10, 1993).
Nuclear Security: DOE's Progress on Reducing Its Security Clearance Work Load (GAO/RCED-93-183, Aug. 12, 1993).
Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking Capabilities Are Limited (GAO/RCED/AIMD-95-5, Dec. 27, 1994).
Department of Energy: Poor Management of Nuclear Materials Tracking System Makes Success Unlikely (GAO/AIMD-95-165, Aug. 3, 1995).
Nuclear Nonproliferation: Concerns With the U.S. International Nuclear Materials Tracking System (GAO/T-RCED/AIMD-96-91, Feb. 28, 1996).
DOE Security: Information on Foreign Visitors to the Weapons Laboratories (GAO/T—RCED-96-260).
Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories (GAO/RCED-97-229, Sept. 25, 1997).
Department of Energy: Information on the Distribution of Funds for Counterintelligence Programs and the Resulting Expansion of These Programs (GAO/RCED-97-128R, Apr. 25, 1997).
Department of Energy: Problems in DOE's Foreign Visitor Program Persist (GAO/T-RCED-99-19, Oct. 6, 1998).
Department of Energy: DOE Needs To Improve Controls Over Foreign Visitors To Its Weapons Laboratories (GAO/T-RCED-99-28, Oct. 14, 1998).
Nuclear Nonproliferation: Concerns With DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists (GAO/RCED-99-54, Feb. 19, 1999).

Mr. UPTON. Well, thank you very much for your testimony. Because, again, you are the only panel, and I am the only current member of the subcommittee that's here and there is no one here really to object, we are going to, though I didn't clear this, Mr. Klink, before, we are going to do 10 minutes of questioning per member. So, that's for the staff to know as well. I am told that the Energy and Environment Subcommittee has now finished its work downstairs, so I presume that other members will come up. So, I am going to put this little timer here and watch it very carefully, before yielding back, as I welcome other members here. By the way, all the members are able to put an opening statement into the record.

I appreciate your testimony, and I, again, very much appreciate the opportunity to look over it through the weekend, when I was in Michigan, and have a number of questions prepared, and wrote down a number of comments as you were testifying, as well. I guess the bottom line for me is, as I begin to look into the situation, you talk about all the numbers of visitors coming in. Can you explain why we let so many foreign visitors into our labs, what the importance is, particularly as we look at Cuba, Iran, Iraq, and obviously China, and the reports that have been in the press? What are the benefits?

Mr. REZENDES. These laboratories do a whole array of activities, including producing nuclear weapons. Some of the basic elements in producing nuclear weapons required high energy physics, and a number of other areas that relate to commercial, as well as just academic, besides just producing nuclear weapons. These laboratories, DOE readily points out, and I agree, have more Nobel Laureates than any place on the planet. So the best and the brightest from the world are attracted to these facilities. If you have an interest in high energy physics, you want to go to Los Alamos and study there, or participate, or somehow get plugged into the research that is going there. And increasingly, a lot of DOE's research and development programs are international. A lot of the equipment that is being built today is being built on a collaborative basis with other nations. So, there is some rational as to why they would want to have them there.

Mr. UPTON. Would it violate some treaty that we might have with some other nation if we were to close the door on some of these foreign visitors?

Mr. REZENDES. I don't know——

Mr. UPTON. I'm thinking about the space station, as an example, where we have a collaborative agreement with a number of different countries looking into that.

Mr. REZENDES. I don't know all the specific treaties we have, but we have a number of treaties that provide exchange of scientists and information. I don't know if there would be a violation that would trigger anything there, but I am sure that we get a lot of positive benefits in having foreigners there, also.

Mr. UPTON. You talked about the percentage of background checks that were conducted, at some point considerably less than 10 percent, even in some cases less than 5 percent. What kind of background—I am familiar with background checks. When I worked at the White House, there was a background check undertaken on me, my staff has had background checks and staff of this subcommittee has had background checks. What is it, exactly, and who does the background checks on these folks, as they try to come to try to get entrance into our labs?

Mr. REZENDES. I believe most of them are being done by the FBI. They would basically identify whether this individual that you are checking has any foreign counterintelligence connections. From DOE's perspective, they say the reason they didn't do a lot of background checks because they had other defense in-depth processes there. Even if they had someone from China who was a spy, for example, they had the physical security at Los Alamos. They also had control over classified information and they had restricted areas, controlled areas, non-controlled areas. They said with this defense in depth, it was not necessary to know whether, in fact, the foreign visitor was a spy. But we have checked each one of these other defense mechanisms, and we found major weaknesses in every one of them.

Mr. UPTON. Well, you talked about, in essence, many of these labs were, once you had access to it, it was an open campus.

Mr. REZENDES. That's correct. I had a quote from one official who said they prefer to have a campus-style atmosphere there.

Mr. UPTON. You indicated that there were 10,000 secret documents that were missing. Do you have any idea what might have happened to them?

Mr. REZENDES. Well, see, we're concerned about this as well. Those 10,000 secret documents covered a whole range of issues, including weapons design. When we brought this to the attention of Lawrence Livermore, they were not too excited about it. They basically told us they thought it was an administrative error, that the documents were not really lost, but that they were just not well accounted for; they may have been destroyed, and just not documented that they were destroyed. However, they did not know that. And, in fact, their own procedures call for some kind of assessment, a threat assessment, as to what has happened here. They took over a year to even begin that threat assessment, to determine what was the real issues there with those 10,000 documents.

Mr. UPTON. You talked a little bit about the computers, and you have testified, I guess, in reports that you looked at back in 1988, 1992, and 1994, that there really was not a division between classified and unclassified. We read in the press, even in the last day or 2, but again last week and again the week before, how Secretary Richardson had, in essence, taken them offline, closed them off, shut them down, whatever he did. They are back online now; I guess that order came forth in the last day or 2. Did they take steps to separate between classified and unclassified in terms of what they did? Did they correct that as they turned them back on?

Mr. REZENDES. I don't know. We haven't been back there recently, but we know that the intent was to do just that, and also to provide training, in terms of how to do that, for the various individuals who work those computers.

Mr. UPTON. One of the things that, as we look back at the years that, apparently, the leaks have been going on, through a number of different administrations, certainly a good number of Secretaries are more anxious to talk to Bill Richardson, who is obviously a new Secretary, a former member of this committee, and someone who is recognized and willing to do something—as we sort of think about the horse is out of the barn, but how do we prevent horses in the future from ever getting out of the barn. You have proposed many things over the years, it seems, as you testified, not very many of them, if at all, were ever undertaken by the former Secretaries of Energy, that were there.

I noted that, in 1997, the Department of Energy only requested $5 million for security for these labs. Do you know if they actually asked for more? Is that what we gave them, or did they ask for more? With the recommendations that you have prepared in your report, what would it cost to bring these labs up to speed, in terms of your recommendations? What is your guess?

Mr. REZENDES. There are internal studies from DOE that have those estimates. In fact, some of the ones we have seen are talking $300 or $400 million to improve security there. But in terms of the $5 million, that was strictly for counterintelligence, and that was in addition to what the laboratory is also spending.

Part of the problem here is that there is no single item in the budget that you can go to that says "safeguards and securities." In essence, each of the laboratories, each of the facilities, use their

funds to employ security personnel, fences, and the kinds of things you would have in a safeguards and securities program. But, that is not a specific line item; so, its very difficult to collect, and go through, all the budgets and try and find out actually how much is spent out there.

Mr. UPTON. Do you think that would be valuable for us to do, to have a line item for counter-intelligence and security for these labs, as far as the appropriations process?

Mr. REZENDES. As far back as 1977, we were recommending that they have an independent assessment, and that independent assessment provide the President and the Congress with an assessment what the security is at these facilities and what it is going to cost to correct it.

Mr. UPTON. I want to go back, again, to the question about the actual background check itself. And I am going to use it in the context of when they did a background check on Fred Upton. They went back, and they talked to my former teachers, they talked to my neighbors, they talked to my roommates, it was actually good to look at the file because I had lost track of a number of them over the years but, they did a fairly exhaustive and thorough review, and I passed, obviously, with flying colors.

But, as you think about folks coming in from other countries, whether it be Cuba, Iraq, or China, there is no way that you can have a similar type check, or even have access to that individual's history. And yet, thousands of folks are coming into these labs, of which 95 percent of them don't even appear to even get a cursory review. Is that—unless someone——

Mr. REZENDES. Yes, you can find stuff. I'll let Jack Schulze, who has actually dealt with the FBI on this issue—but you know, when we actually checked, we found that 13 of those that we asked them to check, actually had connections to counterintelligence. So they keep a data base.

Mr. SCHULZE. Let me clarify what they do regarding "background check." DOE likes to use the term "indices check" and the FBI uses the term "name check." Basically, the name, the place of birth, and the date of birth, is provided to both the FBI and the CIA. They take that information and they go to their files to see if there is derogatory information on that individual. If they do not have any information, they are not going to go out and do another investigation. They just send back to DOE, "We don't know anything about them," and that is the extent of it.

If they have something that is derogatory—it could be that the person is connected with intelligence service; it could be other things that raises concerns, or could raise concerns to DOE—they will transmit that information over to DOE, for them to use in their decision to whether to let this person into the lab or not.

Mr. REZENDES. I think you are asking a process question. I want to make it clear. They are not going to go to this foreigner's school, or talk to his neighbors, as they did in your situation. But, basically, we have our own intelligence networks that are overseas, and are keeping track of what is happening there. To the extent that we can re-harvest that information, we can use it to compare people who come here.

Mr. UPTON. Thank you. My 10 minutes is expired, so I would yield 10 minutes to Mr. Klink.

Mr. KLINK. I ask the chairman unanimous consent that Mr. Stupak be allowed to go out of order. I understand that he has some time constraints.

Mr. UPTON. Without objection, fine.

Mr. STUPAK. Thank you, and thank you Mr. Chairman, and thank you, Mr. Klink, for yielding. Mr. Rezendes, am I saying that right?

Mr. REZENDES. Rezendes.

Mr. STUPAK. Rezendes. In your written testimony, you mention that the DOE counterintelligence program had never completed comprehensive threat assessment. So they really didn't know what threat they're guarding against, or how to concentrate their resources on meeting that threat. In the 20 plus years that GAO has been looking at security and safeguards at the DOE weapons facilities, how many times have you pointed out that comprehensive threat or vulnerability assessments had not been made?

Mr. REZENDES. I don't have an exact count, but I would say several would be probably fair.

Mr. STUPAK. Well, let me list for you a few times that you brought this to Congress' attention and to DOE's attention. I believe it was 1976, 1982, 1988, 1992, and 1997. Now that spans the last five administrations. A period in which the cold war was in full swing, and the period after the end of the cold war. Can you explain to me why DOE, in all these administrations, can't develop a good threat assessment and focus their resources on meeting that threat?

Mr. REZENDES. The only conclusion I can come to is they don't consider it a high priority. They prefer to spend their money on other things other than this.

Mr. STUPAK. Well, you had said earlier in some questions to Mr. Upton, that they thought that security defense in depth.

Mr. REZENDES. Right.

Mr. STUPAK. Explain that. What do you mean?

Mr. REZENDES. Basically, as I was saying, they didn't do background checks on these foreigners on some cases, and sometimes we were told they didn't care if they were foreign intelligence officers because, basically, they had the physical security. They had guards. They had gates there. They were prevented from going into restricted areas. They had control over classified documents. Classified documents weren't just hanging around. But, the reality is, every time we looked at one of those defense mechanisms, we found problems.

Mr. STUPAK. Is that a combination of don't care, didn't know? Or relying too much on the security that was in place? Is it a combination, or is it any one of those three stand out that they just——

Mr. REZENDES. Actually, I think it's even more basic than that. I think there's a culture that exists there of focus on research and openness, and focus on what they're doing, whether its high energy physics or not. But, I think the real fundamental problem is a lack of accountability. We're not holding people accountable, and I think that if we did that, these wouldn't reoccur with such frequency.

Mr. STUPAK. My staff was told yesterday by DOE that a threat assessment involved looking at the entire DOE complex, and vulnerability assessments are those developed for each individual site. Why is it so important to have a threat assessment? Don't people just know what the threats are?

Mr. REZENDES. No. You could have various countries. One country could be targeting, for example, information on electronics on a warhead. Another one could be talking about re-processing nuclear materials. Another one may be targeting actual physical theft of nuclear materials. You would have a different response to each one of those, and those responses would be different at each of the facilities because each one had various duties. One may be more focused on electronics for a specific warhead. Another one may be focused more on re-processing. There could be a number of issues.

Mr. STUPAK. Other than weapons, what else do they produce or research do they do at these labs?

Mr. REZENDES. Oh, great. That's a really good questions, because I think we are focused on weapons. I like to point out that nuclear weapons is yesterdays news. That's 50 year old technology that is delivered on warheads that is really 70 year old technology. The new stuff today is supercomputers. I think we need to be as careful about them as some of these nuclear designs. Not that I'm advocating loosening controls on nuclear designs. But, certainly, I think supercomputers are much more advantageous to our enemies in the future.

Mr. STUPAK. At which one of these labs is the supercomputer research being done?

Mr. REZENDES. Actually, its being done at three of them, but the two big ones are Los Alamos and Livermore.

Mr. STUPAK. Since you moved from, if I can use the word, the old technology of nuclear weapons to the supercomputers, has there been any sense in these labs that, maybe we have to ratchet it up now, now we're into computers and more electronics, that we should ratchet up our security or do a threat assessment on what we're doing in this new phase of work we're doing?

Mr. REZENDES. I don't know, obviously, what's in their head. Most of the kinds of things we're talking to, and I probably should make that very clear, is, we're talking about the processes for actual security, which is the security forces, the background checks, the personnel security checks, that kinds of stuff. The area we've not addressed, and I think its ripe, is what's in people's heads and what they take to conferences, what they take outside the gates, or the conversations they have with other people. That is a much more difficult thing to control, and one we've not addressed in this process.

Mr. STUPAK. Let me ask you this. We're concerned about the security there, and Mr. Upton asked a question back to 1997. Congress gave an extra $5 million for counterintelligence, but yet, when I look at the way that $5 million was spent, I guess I'm sort of bemused. Because if I understand right, the $5 million, only $1.6 million additional went into actual counterintelligence. DOE headquarters kept $1.3 million for studies. The facilities took $1.4 million for overhead, and reduced their own expenditures. The Lawrence-Livermore lab, for example, was allocated the most money,

and put about half of it into overhead, and reduced its previous expenditures.

So, the money didn't go where Congress intended. But, it seems like there is not an appreciation of the sensitivity or the seriousness of the information being dealt with, if I can use the word in the campus atmosphere that you described earlier.

Mr. REZENDES. I think you're exactly right, and I that is an excellent example of the lack of priority that is given to this, specifically at the facilities. When DOE provided the extra money to assist them with counterintelligence, some of these facilities' reaction was to cut their own commitment, cut their own budgets that there were doing, and substituting the DOE money. Obviously, they thought that spending that extra money on other R&D, or other kinds of activities at the facilities, was much more important than counterintelligence.

Mr. STUPAK. I know that we've only had two witnesses thus far, but I do have to run to another hearing. I'd be interested, after your review, after all that has gone on, any other recommendations or—how would you address this lack of sensitivity to this issue?

Mr. REZENDES. Two issues. One, DOE has a very complex organizational structure which makes it difficult to set clear responsibility, which is one problem. Once you establish clear responsibility for having people do something, hold them accountable for doing it. We've not seen that.

Mr. STUPAK. Responsibility and accountability.

Mr. REZENDES. Absolutely.

Mr. STUPAK. How do you deal with the part you point out where a lot of this is in the minds of the people who work there? How do you deprogram that periodically to make sure that those thoughts are not getting away from its intended purpose?

Mr. REZENDES. You have to take very aggressive action when an issue comes up. Make it severe. Make it visible, and make it painful so that everybody understands, so you have created a case example that people can really relate to.

Mr. STUPAK. So, with that would have to be that responsibility and accountability you speak of.

Mr. REZENDES. Absolutely.

Mr. STUPAK. Thank you. I yield back any time I may have.

Mr. UPTON. Thank you. Now that more members are here, we're going to go back to the 5-minute rule. We'll go another round if we need to, for sure. Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman. I won't take that as a subtle hint, I'm sure.

Mr. UPTON. No. No. Not meant that way.

Mr. BILBRAY. I'm looking down at the list of visitors. Didn't anybody even raise a flag when you had, you know, hundreds of visitors from China, Iraq, and Russia? Nobody even raised a flag about that?

Mr. REZENDES. It made us nervous.

Mr. BILBRAY. I would just be very interested in issues like China isn't participating in our international fusion research, the Eter program. What were they interested in? What were the visits aimed at?

Mr. REZENDES. I don't think I have that list. Do we? There was a wide variety of issues. I don't have any specifics for you, though.

Mr. BILBRAY. I'm just interested. I see a lot of the partners that are working with us on the energy projects. Of course, I would question why France isn't on the review process after we've seen some of things that France has done in the past with economic espionage. I'll open that up as a controversy here. In fact, I told the French Ambassador to his face that I was more worried about his espionage than I was about Russia.

Mr. REZENDES. I think you raise a very good concern, because more and more these laboratories' activities are going into applied research and commercialization.

Mr. BILBRAY. I'm glad you reinforced that, because I think too many of us always think about the military application traditionally, and not the fact that a lot of it is economic espionage and then it, de facto, can be distributed through the economic aspect of it.

The report that identified the visitors—Mr. Chairman, I need some clarification. Is the re-classification of the countries in 1994, is that privileged information, or can I discuss it in public?

Mr. UPTON. I'm not sure. The GAO report has a classified and an unclassified version. From where I see what you're reading, that's the unclassified report.

Mr. BILBRAY. Okay. I just want to point out——

Mr. UPTON. 1997, right?

Mr. BILBRAY. Yes. 1997.

Mr. REZENDES. Yes. That's unclassified.

Mr. BILBRAY. It just shows that we've gone from our sensitivity back in 1994 that all these countries need to be re-classified. The countries that we're moved from sensitive to non-sensitive included nations named Yugoslavia, Vietnam, Romania. I'm just worried. Our good intentions are out there much farther than reality is when we talk about who is or who isn't a potential threat. Do you have any comments at all about that aspect of it? The reports that come down don't even include that.

Mr. REZENDES. Exactly. You're right. Who our enemies are and who are friends are changes from year to year, and over decades it becomes more obvious how their shifts are. But, even with our friends, we have to be cautious about what kind of information is out there. Whether its from a defense posture, or whether its a commercial posture.

Mr. BILBRAY. My biggest problem, I've had—my mother was an Estonian immigrant, and she always pointed out that Americans lose the fine line between being the nice guy and being the patsy. We bend over so much to try to be the nice guy that people take advantage of that. Mr. Chairman, I have other questions, but I think that it is quite clear that the new Secretary has quite a lot of work cut out for him, and thank god its the man we know who's up there who's doing it, because I think he can take it on. But, I think it raises major issues that we have to continue to raise, and I don't think anybody in their right mind would look at this and say this is a reasonable way for our Nation's laboratories to be operated, especially with the sensitive issues.

I'm glad that somebody who represents San Diego county—with all our high tech—I'm glad that you highlight that the nuclear

threat is one that the public and the Congress perceives, but it is those threats in high tech that we underestimate, and that is really the cutting edge of our military superiority right now. Not how big a bomb we have, or how fancy a bomb we have, but our ability to get things to a certain location at a certain time. Thank you very much, and that obviously indicates that he's cutting me off.

Mr. UPTON. Thank you, Mr. Bilbray. Mr. Klink.

Mr. KLINK. Mr. Rezendes. I was just thinking that if we handed out an award for the most re-occurring role in this subcommittee, you probably would win it. You've become someone we depend on a great deal, and you always are here, and cooperative, and intelligent, and informative, and I welcome you back again for this Congress.

I'm almost indecisive about how to start the questioning. There is so much material that we need to go through. Let me set the basis for this, if I can, to talk about what, in fact, kind of spying, and what kind of information, and how it may be taken out of these laboratories. I think that a lot of us have grown up on James Bond movies, and we tend to think of spying in that regard. Very overt. It appears to me by what I've read and what I've heard, that this is much less overt. It is, in fact, scientists and others coming from other countries. Some countries that we would be suspicious of, as my colleague Mr. Bilbray said. Automatically when we hear Iraq and China and some of these other countries, the hair on the back of our neck may rise, but, in fact, the worst damage may not come from people from those obvious countries. It may not be leaving in obvious ways. As I said in my opening statement, we're worried about gates and guns and guards. In fact, what we're worried about is what comes out of the laboratories in the minds of our people.

Mr. REZENDES. Correct.

Mr. KLINK. So, it may be private and personal relationships which develop.

Mr. REZENDES. Absolutely.

Mr. KLINK. Which our scientists and others may not even know. They may, in fact, be hapless in knowing that they are victims. These are probably not people who have accepted anything gratuitous. They have not been paid for giving away secrets. But, in fact, once they develop relationships with these people, if, for example, the Chinese were able to get one snippet of information from you, and one from Mr. Boss, and one from Mr. Schulze, and one from Mr. Fenzel, and one from Mr. Upton, and one from me, they go back to China, they put all these information——

Mr. REZENDES. They didn't get it from me.

Mr. KLINK. Now they've got something and we didn't know about it.

Mr. REZENDES. That's true.

Mr. KLINK. What my problem is, is how do we make sure, and I go back to Mr. Stupak's question. In 1997, we gave $5 million more dollars to say, "take care of this problem." Instead, that money went for overhead, it went for other things, and, in fact, if we're just bringing in people and we're giving them 1 to 2 hours worth of training in a year, essentially aren't all we're accomplishing is saying, "here's how you change the password on your com-

puter, and, by the way, put these documents in a safe and make sure the safe is locked when you're not in your office."

What else can we be accomplishing with all of this? I was interested in your 1997 report on foreign visitors where you mention that DOE was trying to improve its counterintelligence program. But, you said that the program would not be funded because of, the quote you gave was, "historical lack of support for counterintelligence programs."

Now, you found that the annual counterintelligence budget was $1.4 million, which put about one person at each facility. What could one person do?

Mr. REZENDES. Not very much. In fact, I can give you an example at Los Alamos. They have one person who is responsible for not only checking with foreign visitors, but also debriefing the thousands of DOE officials and contract officials who go oversees. It was an impossible task. One person could not do all of that.

Mr. KLINK. Other than the chairman holding this great hearing, and us continuing to push, how do we raise the level of this with DOE? Again, going back to another one of Mr. Stupak's questions. You were here from 1976 on through to the present. Five administrations. What in the world can we do to make something happen? We can't wait any longer. The kind of information that we may be losing with both Republican and Democratic administrations, both Republican and Democratic appointed Secretaries of Energy, and the underlings, just continues. Everybody got some share of the blame in all of this. How do we begin to make sure, under this subcommittees oversight, that it ends now.

Mr. REZENDES. Great question.

Mr. KLINK. Give me a great answer.

Mr. REZENDES. Part of it relates to having the correct information, having counterintelligence information, that sort of thing. But then, who gets that? We advocated for over 20 years that there should be some kind of independent source that evaluates what is happening in safeguards and securities at DOE; that they report in a report to the President and to Congress to identify not only what the problems are, but also to address what the recommendations are, and what its going to cost to fix that. We still don't see that happening as clearly as it needs to happen.

Once you have that information, I think what is really incumbent, and what we'd like to see, is you hold the Department of Energy responsible for following through. Put them on a schedule with reporting timeframes back to you. If it has to be monthly, 6 months, once a year. I don't know what the timeframe is. If they're not doing it, hold somebody accountable. Somebody should lose their job if its not done. I think if that message is sent clearly, it will happen.

Mr. KLINK. If I could just ask your indulgence, Mr. Chairman, for one follow-up? GAO also said that DOE has no detailed oversight of the labs counterintelligence programs, performance measures for them, or even periodic evaluation. If that still true?

Mr. REZENDES. That is still true. I know Secretary Richardson and Ernie Moniz, in particular, has been designated by the Secretary—he's the Under Secretary for DOE—has been designated to head up a group to try to clear up these lines of responsibility and

accountability, and also the various offices that relate to intelligence, counterintelligence, and Office of Safeguards and Security, and security evaluation. Those are all separate groups that exist out there. He's trying to make sense of that, and trying to streamline that right now.

Mr. KLINK. Thank you, Mr. Chairman. I look forward to our second round.

Mr. UPTON. Thank you. Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman. Welcome back, Mr. Rezendes. GAO has had prior assessments, as was described by Mr. Stupak. What's changed at DOE that should make us all feel comfortable that the current suggestions by the current Secretary will, in fact, work, or will, in fact, be carried through?

Mr. REZENDES. Despite the negative message here, we're always optimistic when we see someone in a high place take on the problem, and, in sincerity, try to follow it through to make something happen. I think this current Secretary is doing that. However, its still a work in progress. We've seen this before over the last 20 years. We don't know how it will be cascaded down through the infrastructure at DOE, how it will be received, and whether they'll follow through. This Secretary has been here a short time, and will probably be here a short time. The average life expectancy for a Secretary and a Deputy Secretary, and an Under Secretary, and an Assistant Secretary, is probably about 2 years, 2½ years, historically. Not just at DOE. I'm talking about in the Federal Government in general. These contractors have been these for a long time. The University of California has managed, as the contractor, Lawrence-Livermore and Los Alamos for over 50 consecutive years. They have outlasted all the Secretaries of Energy that have come and gone.

Mr. BURR. I probably should ask you some follow-ups about that, but I'd be scared to do it today. Let me ask if you pursued any leads that were the result of whistle-blowers at DOE?

Mr. REZENDES. We do not. We get that information. We use it periodically. We have not frontally addressed any whistle-blower situation as it relates to safeguarding and security.

Mr. BURR. Can you give us any indication as to the atmosphere at DOE as it relates to whistle-blowers?

Mr. REZENDES. Not more than what I hear in the press, and what I hear from whistle-blowers who call me up.

Mr. BURR. Has the GAO reviewed the security of DOE's headquarters?

Mr. REZENDES. Actually, no. I don't think we have, to tell you the truth. Most of the time, we've looked at the most sensitive facilities. I don't think we've ever looked at headquarters.

Mr. BURR. From what you've seen at the facilities, would there be a reason to believe that maybe the headquarters might need a review?

Mr. REZENDES. That's an interesting question.

Mr. BURR. Has GAO reviewed DOD, as it relates to the clearance procedures?

Mr. REZENDES. Yes, we have. In fact, there is a counterpart, my counterpart, that does Department of Defense work.

Mr. BURR. Can you compare the findings of the clearance procedures at DOD relative to what you found at DOE?

Mr. REZENDES. We looked at them a while back, but its been many years.

Mr. FENZEL. There's differences.

Mr. REZENDES. We didn't look, as Mr. Fenzel said. We didn't compare and contrast to see who's doing better, but we did look at the processes that they both use for security clearances a long time ago. We found out that, it was kind of amusing, while they each have security clearance processes and secrets, and that sort of thing, they each define secrets differently, and they each have a different process for clearing people, and those processes—there is very little reciprocity. That was at the time we looked. I don't know if its changed now.

Mr. BURR. Let me ask you. Secretary Richardson, I think, said in front of the Senate Armed Services Committee, that 9 of the 12 weapons facilities are satisfactorily performing their security mission. Do you find that to be a true statement? Are 9 of the 12 free of any security problems?

Mr. REZENDES. We've been asked by this committee to go back and do a follow-up on our recommendations and our reports. We're in the process of doing that. I don't have a status for you now.

Mr. BURR. Can you comment at all on the effectiveness of the Office of the Inspector General at DOE, as it relates to the deficiencies that you found at the DOE facilities?

Mr. REZENDES. The IG is pretty aggressive. He has a wide range of activities with, I'm sure he would say, limited staff. He prioritizes those, and I don't think he's spent as many resources as we have in this area.

Mr. BURR. Do you feel comfortable that he understands the problems that you've identified, and that others have identified at the facilities?

Mr. REZENDES. I'm pretty confident. We meet with him periodically and share agendas and information. I'm pretty confident he has——

Mr. BURR. Given that our concern is with espionage and security right now at these facilities, if one accepts that as the problem and sole problem, how difficult is it to design a system to secure these facilities? Are we talking about something relatively easy, or tremendously difficult?

Mr. REZENDES. The system you would put in place, is probably, on a relative scale, closer to the easy side. The difficulty is assuring yourself, ever having a high degree of confidence, that there is never going to be a breach. I think, historically, we looked over the history, we've seen a lot of the breaches, or some of them, anyway, have come internally. For example, during the Manhattans projects, you had Carl Fukes and the Rosenbergs. That was an internal breach of security. The Rosenbergs never broke into Los Alamos. I don't even think they received secret documents from Los Alamos. I think the people who worked there brought them out and exchanged information from what was in their head, rather than breaching some of the security defenses.

Mr. BURR. Let me ask you, and I ask the chairman for patience. You mentioned earlier the knowledge that's in the heads of individ-

uals, versus the sensitivity of bringing documents out. Match that, if you will, with this new tool called the supercomputer, and make the connection for everybody here as to where the knowledge of the head and the supercomputer come together, and why that should be a risk.

Mr. REZENDES. I think that is a really good example. I think its easy for researchers who are going down this road, who understand that supercomputers have a defense benefit, but also, are confronted with the calculations and the difficulty and the science of doing it, and getting together with other scientists who share those same concerns, and also have interest.

It is easy to subdivide a problem so its so small that you can lose track that its going to have anything to do with national security in the future. That's why counterintelligence and threat assessments are really important. If you knew that some of our allies or some of our enemies were targeting information on supercomputers, and were also going to do it on a piece by piecemeal basis, as Mr. Klink said, rather than try to sneak in and steal documents, the strategy you're going to use to protect that information from a defensive perspective is going to be different, and that's the kind of thing we'd like to see DOE do.

Mr. BURR. Doesn't, in fact, the supercomputer and the knowledge that's readily available in people's heads, doesn't that really bypass the need to steal the secret, because you can recreate what the secret was? You can refine the step that it was at?

Mr. REZENDES. That is correct.

Mr. BURR. Without active testing?

Mr. REZENDES. Not easily, but you can do it.

Mr. BURR. Can you define supercomputer for us?

Mr. REZENDES. Oh, sure. Supercomputers are state-of-the-art computers that DOE is currently developing, and these will do calculations at variable speeds. These things have never been developed. They've never been built. None exist on the planet, and probably won't be, even by DOE's schedule, for years to come. These will be able to, once their operational, to replicate what happens during a nuclear explosion when there's countless different equations that need to be taken into consideration.

Mr. BURR. And we're not talking about an off-the-shelf computer?

Mr. REZENDES. This is the first of its kind.

Mr. BURR. Even with the advances in chips as we move into next year with the new chip.

Mr. REZENDES. Correct.

Mr. BURR. They're no where near.

Mr. REZENDES. Correct. This is the first of a kind.

Mr. BURR. All right. I thank the chairman.

Mr. UPTON. You're welcome. Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I apologize for being late and not hearing all of your testimony. I have read most of it. Would you say, obviously, over 20 years, there has been oversight from GAO with very little luck. Is it a systemic problem with Department of Energy? They don't have a priority on the security issue?

Mr. REZENDES. I would say they certainly don't have a priority. It's been low priority and low visibility.

Mr. GREEN. I know that the role of the Department of Energy is research, and not necessarily security. It is this Congress that would make the decision on whether the Department of Energy needs to continue that without some oversight from someone who is more security minded, like a military or NSA or someone like that. I know that the decision was made long before we got here that the Department of Energy would do that research. It seems to clash with their campus and their free-flowing ideas that they have on their facilities. Security doesn't match their original goal. It seems like, Mr. Chairman, what we might need to do is, fairly quickly, and I know that the Secretary and his staff have testified in the Senate, but have the Secretary come after a reasonable time and give us some goals and objectives, and then within the next year have another hearing just like this with the Secretary and maybe a follow-up GAO report. So, for the first time maybe in the 20 years, we can see that say, okay, if you didn't complete it this year, what can you do? You took $5 million in 1997, not this current Secretary, far be it for me to speak ill of my current friend, but you spent $5 million from 1997 and used it for, obviously, other things other than security, and now you want $40 million? What can we know that will be done what that? I think that, Mr. Chairman, is probably what we need to do.

Let me ask a line of questions. I hope that we would follow-up fairly quickly with Department of Energy coming——

Mr. UPTON. Let me just tell my—and I'll stop the clock here, like any good line judge. We are intending to do a number of hearings. One of the things that we would like to wait upon, however, and we'll see what happens, particularly in calling our friend, Secretary Richardson, to come, is we're trying to see when the Cox report will become more available or unclassified. I guess there was a little glitch over the weekend, so we'll be checking with Mr. Dicks and Mr. Cox this week. But at some point, likely sometime early in May, we intend to have the next hearing. We may indeed have a number of these.

Mr. GREEN. I agree, obviously, we'd like to have the benefit of that report, but it also seems like this is a 20 year problem, whatever the report says, we need—our job is oversight on the Department of Energy—we need to follow up and see if we can stop this 20 year trend of saying yes to the problem, and then nothing being done on it. So, that's why I say hold the Department accountable for some security oversight, and raise it on their priority level, whether it's funding, or whether they have to come back before this subcommittee or some other committee on a regular basis to justify it. Again, it bothers me, because it seems like it doesn't fit in with their original mission for research. They want to share ideas and research. Sometimes it's not security oriented, but we do have agencies of the government that have a security interest in mind that could always oversee it.

Mr. REZENDES. Well, you raise an interesting point. The Department of Energy has recast itself significantly over the years. Initially, it was the Department of Energy that was responsible for producing nuclear weapons. Then that switched. Actually, it started off as the Department of Energy to address the energy crisis, the oil crisis at the time. Then it became——

Mr. GREEN. They haven't solved that problem either.

Mr. REZENDES. Right. Then most of its money went to producing nuclear weapons in the early 1980's. And then it switched to an environmental restoration agency, and cleaning up the mess that they made when they were producing nuclear weapons. And now they've recast themselves again into a department of science. In fact, they claim they have four basic missions. One is a defense mission, an environmental. management, restoration mission, an energy mission, and a science mission. And each of those has different priorities, and I think they certainly impact on the point you're trying to make in terms of how they do the research at these facilities.

Mr. GREEN. And there have been efforts over 20 years. I know that one of the reports showed 12,000 documents, and they found 2,000 documents, but there were still 10,000 somewhere that they couldn't find. But that's my concern. A number of times over the years, GAO has pointed out to Congress the safeguards. One example is GAO finally agreed in 1988 to develop a comprehensive security plans for its sensitive sites, and it took more than 40 years to do it again. According to GAO, because of lack of a management commitment, and again, that's our job to try to instill that management commitment. Are you even saying, and I hate to mention former Secretaries, but former Secretary Watkins, who probably gave security more attention than any other Secretary in the 1980's, still didn't provide sufficient resources either to headquarters, to follow up my colleague, Mr. Burr, or in the field?

Mr. REZENDES. Well, what happens is, as I mentioned earlier, even if the Secretary decides to give more resources, it always doesn't happen. There is not a specific line item throughout the DOE budget, for example, Los Alamos gets a billion dollars to run that facility. They spend it on a whole variety of issues, of which one piece would be safeguards and securities, and they have wide flexibility in terms of deciding how much to allocate for that effort.

Mr. BURR. Would the gentleman yield for 1 second?

Mr. GREEN. Be glad to.

Mr. BURR. Is that decision made at the Secretary level, or is it made at the lab?

Mr. REZENDES. The implementation is at the lab. I don't even know, in fact, I don't think that its ever rolled up to the Secretary level, how much is actually being spent, by facility, on safeguards and securities.

Mr. GREEN. Mr. Chairman, we are not the appropriations subcommittee, but we have some responsibility, and I think, again, to follow-up on this report, and see if we can instill in the Department of Energy that they also have a security concern.

Mr. UPTON. I think that's a very good idea. If the appropriations committee doesn't do it, we'll do it for them. Ms. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman. I have a number of questions on foreign visitors and the background check program. First of all, how many cases are you aware of where foreign visitors to the labs have actually obtained classified information?

Mr. REZENDES. We are aware of some. Some of those are classified.

Mrs. WILSON. I'm not asking you for the cases. I'm asking you how many cases you are aware of.

Mr. SCHULZE. We know of some instances where they—we're not talking about theft of classified information—but where they were inappropriately provided unclassified information. There are some situations at Los Alamos where they were provided classified information in newsletters. They were put on a mailing list, and they shouldn't have been, and they got this classified information. Some of these people also were from sensitive countries. Additionally, they would attend various briefings and got classified information.

Mr. BURR. Would the gentlewoman yield for a second? Did I just hear you say that we mailed classified information?

Mr. SCHULZE. It was internal in the laboratory.

Mr. REZENDES. Right. They were just part of the distribution list, and they should not have been.

Mr. BURR. Can you define a distribution list? I mean, are we talking about e-mail, or are we talking about hard copies?

Mr. SCHULZE. In this situation, I would imagine its hard copies. I can't tell you specifically. I could provide that later. I imagine it was by hard copy of a newsletter within a group. We're not talking about something that was laboratory wide.

Mr. BURR. But I also get the impression that we're not talking about something where there was a record kept of the number of copies that were produced.

Mr. SCHULZE. I can't answer that.

Mr. REZENDES. Getting back to the substance of your question, if I may. We're probably the wrong ones to ask. We would not normally be privy to that information. That is something that the FBI would be the ones, if it were available and its known, they're the ones that would be investigating and keeping that information.

Mrs. WILSON. Nonetheless, you've come up with a conclusion that raises serious questions about the foreign visitor program at the lab, and without knowing whether any damage has been done, I don't know how we can come up with——

Mr. REZENDES. We have damages. We have things done. We have people who have confessed to disclosing classified information from the laboratory.

Mrs. WILSON. To foreign visitors at the laboratories?

Mr. REZENDES. Correct.

Mrs. WILSON. What percent of the foreign visitors do the nuclear weapons labs actually visit the limited secure areas of the labs? I'm not talking about the solar cells or the engine lab, or the environmental restoration aspects. What percent of the foreign visitors visit the nuclear weapons——

Mr. REZENDES. We asked DOE that, and they estimate about 10 percent.

Mrs. WILSON. Who estimates 10 percent?

Mr. REZENDES. DOE.

Mr. SCHULZE. You mean actual classified in the secure areas?

Mrs. WILSON. In the limited secure areas of the lab.

Mr. REZENDES. I'd say 5 to 10 percent, I think is what they told us.

Mrs. WILSON. And are those visitors escorted at all times?

Mr. SCHULZE. In the secure areas.

Mr. REZENDES. They're supposed to be.

Mrs. WILSON. Did you find any evidence that those visitors to the secure area of the labs were not escorted?

Mr. REZENDES. We did not check for that.

Mr. SCHULZE. The work that we were doing, we were looking on the unclassified side. We collected information on that, but we didn't do a detailed look to see what happens when people go into the secure areas. I do know of an example of where a foreign national did get in a secure area, and he wasn't supposed to be in there. That has happened. In that case, the person even came in with a camera.

Mrs. WILSON. You talk about the number of foreign visits per year, and they average about, as I do the math here, about 2,000 per year at all three of the weapons labs. How does that compare with foreign visitors to DOE headquarters?

Mr. REZENDES. We don't have those numbers.

Mrs. WILSON. How about the Old Executive Office Building and the White House complex?

Mr. REZENDES. I have no idea.

Mrs. WILSON. How about the Pentagon? I think you get my point here. Foreign visitors and physical theft may not be the major threat here, which gets back to my issue of what we're looking at, what we can see in our narrow little flashlight, and we're likely to miss——

Mr. REZENDES. We totally agree with that, in fact, I often use the analogies of what we're talking about here is in home security of the door locks, the window locks, and that sort of thing, but it doesn't necessarily prevent a burglar from coming in. But, the other side of that is, you don't want to sleep with your door open. You want to have some basic minimum systems in place and those should be effective.

Mrs. WILSON. Thank you, Mr. Chairman. I have additional questions when we have time.

Mr. UPTON. Mr. Klink.

Mr. KLINK. Thank you, Chairman. In GAO's 1998 testimony before the House National Security Committee, you stated that sensitive subjects such as the detection of unsanctioned nuclear explosions may have been discussed with foreign visitors without DOE's knowledge or approval. Let me ask you, what is the process in place to control information about items that might be sensitive, but would not be classified?

Mr. SCHULZE. Discussing a sensitive subject is permissible. I mean, it can be done. DOE wants to be notified of the visit, what the subject is going to be, and where DOE can make a decision as to whether they want that to occur or not, or whether they want to put limits or restrictions on what's going to be discussed.

Mr. KLINK. How do we know if that's happened? How does DOE know if that's happening? How does GAO know that's happening?

Mr. SCHULZE. For DOE to know that its happening, the host of the visit has to identify the visit as involving a sensitive subject. When the host says this is a sensitive subject, then it kicks it into a different category. They have to notify DOE. It goes into headquarters where people in the office of non-proliferation of national

security look at it, and make a determination as to whether this should occur.

Mr. REZENDES. This gets back to your point earlier about this one person in counterintelligence. That was his job, to be aware of those visits, debrief, and also to debrief the contractors in DOE going overseas. These were thousands of visits. It was impossible for one person.

Mr. KLINK. The other point is, what I went back to, is what happens is that there become personal relationships.

Mr. REZENDES. True.

Mr. KLINK. My question is, what criteria are there that the host who's responsible for making the report, would, in fact, recognize immediately that this was sensitive information, and would report it as such, or think this is my dear friend who I've met with dozens of times and we, of course, have shared information about these things. What is releasing information that shouldn't be released, and what isn't, and who's responsible for knowing it?

Mr. REZENDES. No, you're right, and although there is a process in place, I think the onus is on the individual who is hosting the visit, and if this personal relationship develops, as you mentioned, I doubt they're going to be as aggressive in notifying ahead of time the right authorities what the meeting is going to be about, and what's going to be discussed and debriefed at the end.

Mr. KLINK. Describe for the subcommittee what training these hosts would have to be able to report these things, and to be able to recognize that sensitive information was being discussed.

Mr. SCHULZE. Basically, I'm going to make a few inferences based on talking to counterintelligence folks at the laboratories. They're going to have training courses. That is one of the responsibilities of the counterintelligence——

Mr. KLINK. Is that going on now, do you know?

Mr. SCHULZE. It was being done even when we did our work. The problem is, when you have one person doing it, who is also responsible for looking at all the visitors coming in, and briefing and debriefing everyone on travel, and trying to conduct awareness activities, and make people aware of counterintelligence and the threats against them, its pretty tough. They just couldn't get around to——

Mr. KLINK. And that gets back to our 1 to 2 hours per year, per person.

Mr. REZENDES. Right.

Mr. KLINK. Physically, its impossible timewise, to do this. So the question is, do you now think that DOE has a long-term commitment to fixing these problems?

Mr. REZENDES. As I mentioned before, we're always encouraged. We've seen a laundry list that the Secretary has announced, and he's established a high level commitment within the Department, with Ernie Moniz heading this up. We're encouraged.

Mr. KLINK. I mentioned a little earlier about the administration proposing that we spend $40 million more, and I said, and I mean it, we don't want to see this as just throwing money at a problem. We've already talked about how the $5 million was spent. I'm not real comfortable with the idea of what they might do with $40 million. On what basis do you think that $40 million would be spent effectively? What guarantee do you give to Mr. Upton, Mr. Klink,

and the rest of us that, in fact, there's safeguards in place to make sure this money is going to be spent to do what we all want it to do.

Mr. REZENDES. I would have no commitment to you on that, only a pledge that we would follow up to make sure that they did.

Mr. UPTON. I'm glad you remembered you're still under oath.

Mr. KLINK. There are so many things. I think that the best thing right now, Mr. Chairman, would be to submit some of these questions in writing, because we've barely, as with the training that the people at these labs are getting, we've barely scratched the surface, and I think we would like to have a lot more. I would anticipate too, Mr. Chairman, that this is not the last of our hearings on this subject. I thank you for your patience.

Mr. UPTON. You are indeed correct. Thank you, Mr. Klink. A couple of questions I still have remaining, and again, I may send some things written as well. You talked a little bit earlier about computers still being an open issue. Are there other open issues still unresolved, either in your testimony, or that DOE ought to be looking into, that you've not addressed?

Mr. REZENDES. Sure. In each of the areas that I went to through, everything from material accountability, in terms of being able to inventory and verify nuclear materials. From what I understand, DOE's own internal evaluation groups still raises that as an issue today. I think there's still questions about the guard service, in terms of their skills and abilities. Personnel security. We thought a lot of that had come under control, with the backlogs eliminated, but I'm hearing from some sources, that the backlog is back up again in terms of taking 6 months to a year to do a security clearance before you can get it kicked off. So, I would say every one of those areas, and that is one of the things we plan to do for you as part of that request.

Mr. UPTON. Now one of the questions that we're going to have to ask Secretary Richardson when he comes, hopefully next month as these hearings continue, is certainly the worth and the value of the visitor program, particularly as they have access to both classified, but even sensitive, materials, and knowing full well that its going to take a lot of money and some time to put the systems in place that you recommended, and you recommended over the years.

What would be the harm, at least in the short term, of blocking access, all access, to the sensitive material, as well as the classified material until these safeguards are, in fact, in place. Knowing full well that they may take at least a year to give the training, and put in some of the other safeguards that you've indicated.

Mr. REZENDES. I really don't have a reaction to that. I'm sure DOE would, because they would know what they're giving up.

Mr. UPTON. I think there's actually a bill that's been introduced by one of my colleagues, that would, in fact, do that.

Mr. REZENDES. On the other side of that, and I'm sure DOE would like to give you an answer on that, but we also get access to foreign laboratories and facilities. I don't know what kind of repercussions that would have. In fact, we were half joking saying, "Maybe the real story here is that DOE is getting more out of spying overseas than the spies are getting out of here."

Mr. UPTON. From our folks going over there. You referenced a few minutes ago to Mr. Burr, about California, and some of the universities there, being there for more than 50 years. What type of contract or accountability do you think we ought to put into place? That clearly ought to be one of the areas. Is there no contract or accountability now? Virtually none?

Mr. REZENDES. Basically, we've talked about, particularly with that contract, lack of specific performance measures as they relate to counterintelligence, and they're still not there, and we recommended, I think, in the early 1990's. Let me give you an example here. When Secretary Pena was there, he had a problem at Brookhaven National Laboratory. Brookhaven had a facility there that was leaking tritium into the groundwater, and, basically, the Secretary said that the local community in New York, had lost confidence in that contractor's ability to operate that facility effectively. As a result, he fired that contractor. To make them an example. To set a clear message that when somebody does something that he considers significant, he was going to take aggressive action.

The other side of that is they had the Chicago operations office with 40 people onsite, which were the DOE eyes and ears to make sure the contractor was doing what they were supposed to do. He did the organizational equivalent of firing the Chicago operations office by having those folks report directly to him, rather than Chicago operations office. We went back there later, and we found that, although they were technically reporting to the Secretary, they were still reporting through the Chicago operations office. That office was still responsible for doing the evaluation of the contractor, and monitoring them every day to make sure that they were doing what DOE wants to do. This gets back to my point of responsibility and accountability. It doesn't seem to, when something happens, even severe enough to fire the contractor, the rest of the organization seems to stay in place.

Mr. UPTON. Of the foreign visitors that continue to go to the labs, about what percent of them actually have access to classified or sensitive material? Do you have any guess?

Mr. REZENDES. Well, this gets back to, I think, apparently 5 to 10 percent, we were told by DOE, actually get into restricted areas, and where there is classified information. I don't know how many physically get secret documents or whatever. I don't know.

Mr. UPTON. Mr. Schulze?

Mr. SCHULZE. Is your question how many legitimately get classified information?

Mr. UPTON. Yes.

Mr. SCHULZE. There are some that occur primarily from countries such as United Kingdom, NATO members. Those are classified visits, those do occur. But, those are relatively few in number. We did not look at those.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman. As we speak of responsibility and accountability, I want to go back to the independent evaluation office. I believe it was back in 1977, GAO recommended DOE set up an office of independent evaluation of the line programs to assess safeguards and securities. It made recommenda-

tions in 1983, and I know Mr. Dingell, when he was Chairman here, and this committee attempted to accomplish the same thing by legislation in 1983, but it was opposed by DOE, to put in this independent evaluation office that would report directly to the Secretary. The purpose of the GAO recommendation, I believe, was to make sure that problems were not hidden from the Secretary, and that adequate funding for safeguards and securities was obtained. Am I correct in that?

Mr. REZENDES. Yes. Actually, it was beyond the Secretary. It was also to the President.

Mr. STUPAK. Secretary and the President?

Mr. REZENDES. Right.

Mr. STUPAK. I believe that is what the 1983 legislation recommended. From what I understand, this was never done, either legislatively or within the internal structure of DOE.

Mr. REZENDES. There were changes made. In fact, at that time, we were recommending either one of two options. Either the Nuclear Regulatory Commission take responsibility for this, or that an independent group that was separate from the programming group that had responsibilities for carrying out the safeguards and securities, which in this case, was defense programs, and report directly to the Secretary, or someone else, so they could have this independent oversight. That did happen. In fact, initially, this evaluation group was under the defense programs, which also had responsibility for running the laboratories, which was the concern. They were eventually moved out, as to where they are now under Environmental Health and Safety, where they report to the Assistant Secretary there, which reports to the Under Secretary. So, there is some of that. While they're reporting on the kinds of findings they identify, security and safeguard issues, they don't get into the budget issues as much as the violations.

Mr. STUPAK. Was it truly independent? With that independence, then could they go directly to the Secretary, or was there always an Assistant Secretary, or could they go directly to the President, as recommended in the 1983 legislation?

Mr. REZENDES. I think this has always been through an Assistant Secretary, Environmental Health and Safety.

Mr. STUPAK. The office of security evaluations is the office that reviews the status of safeguards and securities, isn't it?

Mr. REZENDES. That's correct.

Mr. STUPAK. Is it safe to say that, I think you said, the Environment, Safety, and Health division——

Mr. REZENDES. Environmental health and safety.

Mr. STUPAK. Okay. That's not one of the more prominent or potent or powerful divisions within DOE, is it?

Mr. REZENDES. They do a lot of the environmental restoration, environmental management, the health issues. They're a good chunk of DOE's budget.

Mr. STUPAK. But within the DOE culture, if you will, they're not one of the more forceful ones?

Mr. REZENDES. I see what you're saying in terms of, do they have any more clout that anybody else? No.

Mr. STUPAK. I'm still stuck when I asked my last set of questions about don't care, don't understand, or rely to heavily on so-called physical defense systems that's going to protect us.

Mr. REZENDES. Right.

Mr. STUPAK. It seems that there's no appreciation of what we're doing, what we're dealing with. No one really wants to push forward directly to hold people responsible or accountable, to use your words. While there's been some cosmetic things done in the past, that direct line for the accountability, for the responsibility, seems to have never really occurred. I guess that's what I'm trying to get at, and if I'm wrong, let me know.

Mr. REZENDES. Oh, no. I think you're exactly on track. I think if you look at the organizational structure the way it is now, both in terms of the organization of the various elements that have responsibility for safeguard, security, counterintelligence, intelligence, they are diffuse throughout DOE. There isn't unity. In fact, you have various offices that have responsibility for establishing standards, and another group responsible for assuring that standards are being met, but no one has the authority to make sure that these recommendations are, in fact, accomplished. In fact, even the office of safeguards and security evaluations, which does these oversight things, they always make recommendations on things to do. But they don't have any force to make sure those recommendations, in fact, are implemented.

Mr. STUPAK. Thank you.

Mr. UPTON. Mr. Burr.

Mr. BURR. Let me ask, are anyone of you aware of a 1997 directive that may have provided for clearance from one agency, say DOD, to actually carry over to DOE? Possibly a Presidential directive that required the agencies to have a mutual clearance process?

Mr. FENZEL. There were some efforts. When we looked at that situation back in 1995, there were different procedures, and actually different clearances in place, if you worked at DOD as opposed to DOE. The two agencies were working together so they would share their clearances. If you were cleared by one, you would be cleared by the other. But we have not looked at whether that's full cooperation in regard to those clearances. But, I know the two agencies were working together to try to correct that situation.

Mr. BURR. Let me go back to the question of contractors. How does DOE go through the process? We talked about, what was it, University of California?

Mr. REZENDES. Right.

Mr. BURR. How are they chosen? Do they go through a bid process?

Mr. REZENDES. No, they don't. Actually, the University of California was selected during the Manhattan Project in the 1940's to run Los Alamos and Lawrence Berkeley and Lawrence-Livermore. DOE went through a contract reform a while back. One of the objectives of the contract reform effort was that DOE should have more competition, that they should open these up. The University of California, as I said, has managed these facilities for 50 consecutive years without that contract ever being re-competed. DOE has successfully re-competed a lot of contracts, including other facilities that do lab-

oratory research for them. For example, Sandia, Oakridge National Lab are run by private contractors.

Mr. BURR. They never re-competed that particular lab?

Mr. REZENDES. Correct. In 50 years.

Mr. BURR. Has it ever been recommended by GAO or any other——

Mrs. WILSON. Would the gentleman yield for a moment? Sandia National Lab has been re-competed, and was 6 years ago. Los Alamos and Livermore have not, but many of the other national labs have.

Mr. REZENDES. That's correct.

Mr. BURR. Has there ever been a recommendation for Los Alamos?

Mr. REZENDES. We've advocated that DOE use more competition, and that they re-compete as many contracts, or all the contracts, including the University of California contract. It comes up for renewal every 5 years.

Mr. BURR. Let me ask you. Given that you have a Secretary committed to address the security breach that you have identified, that GAO has identified, how long should the Congress expect a serious effort to take before we could turn to a review by GAO that says we have plugged the problem, that we've made tremendous progress in a quantitative way?

Mr. REZENDES. Soon. I would say real soon. At this committee's request, we've started that work already. We'll be reporting back soon. We would expect to see results now. We're just talking about the guns, guards, the process that's in place. We have other folks who are out there. Senator Rudman is looking at the system-wide security issues, and will be coming out with a report within 60 days. I know that the FBI is looking at various issues, and so is the CIA. I think once we see those, then we know specifically what kinds of threats or breaches have occurred, and then we can make a better judgment as to whether we have all the fixes in place that we need to.

Mr. BURR. Thank the chairman. I yield back.

Mr. UPTON. Thank you. Mr. Bilbray.

Mr. BILBRAY. Mr. Chairman, I want to ask this question, and I don't mean it to sound partisan because I think that the problem that we've identified is, what we would call multi-generational, in a lot of ways. But, I'm wondering on the flip-side, we so often talk about the governments. I'm kind of concerned about, have we identified in here the possibility that the business activities may be a major problem here, or representatives of different business segments? There's been concerns about the influence of foreign investors and foreign businesses in our political process, and there may be some nexus between contributions and access to certain issues. I don't want to identify or suggest solely this administration, but can we identify to any degree that the business community wanting access into these laboratories, and foreign business entities gaining access to these facilities?

Mr. REZENDES. Well, I can tell you now. If you go down the list of who is having access to these, these are the numbers of visitors to these, and the numbers with actual working relationships with DOE is big. Thousands. I don't know if I could put a number on

it right now. I think each of the laboratories throughout the weapons complex have collaborations. They have cooperative research and development agreements with the private sector. They have wide open use of a lot of their facilities, both in terms of using the extraordinary equipment that's there, a well as working with the scientific brain trust that's at these facilities to help solve economic problems for businesses.

Mr. BILBRAY. I just think that we need to learn from past mistakes, no matter who did it. We need to start developing a system, and making sure that access to information or access to facilities are based on good policy, and there's going to be some political influence there. We just hope that that political influence has not been unduly influenced by political participation, you know, and contribution. Again, that is not just something that has happened recently. I think its something that's inherently a problem in our whole structure. Thank you. That's all I have, Mr. Chairman. I yield back.

Mr. UPTON. Ms. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman. You note in your testimony that DOE granted Los Alamos and Sandia a waiver on the requirement for the background checks, the indices checks, or names checks, as you call them, on foreign visitors. Was this a comprehensive waiver covering all foreign visitors to the laboratory, or was it a limited waiver, and if so, how was it limited?

Mr. SCHULZE. I'm trying to remember all of the specifics. If somebody was still discussing sensitive subjects or going to a secured area, they still had to get the background check and notify DOE. But, for the most part, most visitors did not have to get a background check. They did not have to notify DOE, or do the other background check requirements.

Mrs. WILSON. So, the waiver only applied to visits of short duration and outside the limited area?

Mr. SCHULZE. Not necessarily. It could be an assignment. There are a lot of assignments that would not be a security area.

Mrs. WILSON. Let me make sure I understand. If they had a waiver, and they could allow foreign visitors outside of the limited area, is that correct? They still require DOE approval to go inside the limited area?

Mr. SCHULZE. There's a secure area, there's a limited area, and there would be an open area. All of the labs have different terminology, but, for the most part, the secure area would be where you did your nuclear weapons work, where your classified information would be. Then you have a property protection area, where sensitive activities could be conducted. Maybe not classified, but things you do not want everybody just to have open access to. Then there would be other areas, which would be considered their open areas. Those areas would be the libraries, cafeterias, a few auditoriums, and those kinds of things would be open areas.

Mrs. WILSON. Let me make sure I understand. Exactly how was the waiver limited? What was the policy guidance from DOE?

Mr. SCHULZE. The policy guidance, essentially, let's use an example. If you were an assignee going to a limited area——

Mr. REZENDES. Assignments are those who are there over 30 days.

Mr. SCHULZE. That normally would require a background check in from a sensitive country. You wouldn't have to do that under the waiver, Its limited to sensitive subjects and security areas, which very few sensitive subjects were identified, and very few security areas.

Mrs. WILSON. You may want to go back and check with DOE on exactly the policy guidance. As I understand it, anything longer than 30 days did require a background check, and anything that was within a limited area also did.

Mr. SCHULZE. We will double check, and I'll get back to you on that.

Mrs. WILSON. I appreciate that. With respect to the indices checks, or the name checks. What did they really provide in terms of value to the laboratory? What does it tell you?

Mr. REZENDES. I can respond to that. Basically, if you have somebody who is affiliated with a foreign intelligence organization, and particularly if you have a counterintelligence threat assessment that you know what they're interested in, you can control who they're seeing. You might want to provide additional escorts. You may want to control the areas that they're going into, and the topics that will be discussed.

Mrs. WILSON. So if a visitor passes that check, it doesn't necessarily mean that they're not gathering——

Mr. REZENDES. No. Absolutely. You're right.

Mrs. WILSON. In your testimony, you say that DOE procedures lack clear criteria for what is and is not sensitive, and therefore, sensitive subjects may have been discussed. Did you discover any evidence that sensitive subjects were discussed?

Mr. SCHULZE. What we found was items that were on DOE's list as being a sensitive subject were the exact things that were listed on the paperwork as the subject of the visit. So, at that point, the host is to notify DOE of the subject, and DOE will make a determination whether its okay or not okay. But things like inertial confinement of fusion were on the list. Inertial confinement of fusion was discussed. Metals like beryllium, which is used in weapons. That was on the list. A visit was discussing beryllium. Detection of nuclear weapons tests was on the list. A visit involved detection of nuclear weapons testing. There was one to one, it was identical.

Mrs. WILSON. Mr, Chairman, may I ask one final question? The Department of Energy, last year, rated Los Alamos National Laboratory as excellent in safeguards and security. Am I correct in assuming that you disagree with that assessment?

Mr. REZENDES. I don't know if I disagree. There was two basic ratings; ones for 1997 and 1998 in terms of safeguards and security. The interesting thing here, and this is the thing where you get back to holding people responsible and accountable. Los Alamos had 45 major security violations in 1998. Some of those, unrelated to the current instances, involved two people being fired, and two of them still under investigation by the FBI for possible criminal violations. If you look at what was happening in Los Alamos prior to that, the typical year for them was about 20 violations per year. Despite the sensitivities, despite the high number of violations, despite the fact that some of them were rather severe, DOE still gave

that contractor an excellent for overall performance on its contract for year.

Mrs. WILSON. And do you disagree with that?

Mr. REZENDES. I'd say that I find it hard to reconcile those two pieces. Yes, I do.

Mrs. WILSON. Thank you.

Mr. UPTON. Thank you. Mr. Klink?

Mr. KLINK. I just wanted to follow-up, and I don't want to get into—I just don't understand the gentlelady's last question, because we have the annual report of the President of the United States on safeguards and security domestic nuclear weapons facilities, and under Los Alamos it says—this is for January 1, 1997, through December 31, 1998—it says marginal, roman numeral II–4. Your question about the excellent rating for Los Alamos. The report that I have is dating January 1, 1997 through December 31, 1998. I want to make sure we're talking about the same things. Prepared by the field operations division, office of safeguards and security, office of securities affairs, roman numeral II–4. At the top, Los Alamos National Laboratory, Albuquerque, New Mexico, overall facility rating, marginal.

Mr. UPTON. Mr. Chairman, I'm talking about a different report. Its the DOE's annual contractor assessment of Los Alamos National Laboratory security and safeguards program.

Mr. REZENDES. Yes, and if I could add something. There was the original reports looking at safeguards and security. When they rolled this up to the overall performance for the contract for the safeguards and security for the year, they gave the contractor an excellent rating.

Mr. KLINK. I just wanted to make sure—which one's real? Is it marginal or is it excellent?

Mr. REZENDES. Well, I think you already have my answer, I can't understand how they get an excellent with the kinds of problems that they've had there.

Mr. KLINK. We've got some questions, and we need to follow up on that, because I think we're all confused. Back in the 1980's, GAO mentioned in the report that threats from insiders were often ignored. I want to get back to this point, because I don't think you can make it enough. All of the alleged breaches may have come from insiders, not outsiders. We don't have, to my knowledge, evidence that computers were breached, that guards were overcome by terrorists, or burglars, or thieves, that gates were broken down, that classified documents were stolen. Again, I guess the question is, what was taken out of the minds of the scientists at these national laboratories? I think this, again, seems to be the most important aspect of counterintelligence and espionage programs.

I suspect, again, with the discussion that we had about the $5 million and how it was spent, and the $40 million. If we're not training these scientists to know what espionage to all about, and its not James Bond sliding in and stealing something surreptitiously, but its about an innocent conversation where you're giving up information, and it does not appear to me, even though in the letter we stuck in the record today from Secretary Richardson, he says that security training is underway to educate personnel on intelligence gathering activities of foreign interests. He said he's

initiated a department-wide polygraph program to weed out potential counterintelligence programs. If a scientist or someone else who's an employee there doesn't know that were a hapless or witless victim in the stealing of information from their minds, not from their computers, not from their files, then how are they going to fail a polygraph?

Mr. REZENDES. No. You're right. There's two elements there. One is, was the scientist duped? Did you know that he was culpable, or was he culpable in terms of the breach of security, or second, was he really just providing information that he thought was not a breach of security?

Mr. KLINK. Mr. Chairman, I share the concern of some of the members on both sides of the aisle that we have to be worried about who has access to these laboratories, who's going in there, but also, if we're going to give them resources, those resources have to be used not only to build higher gates, better gates, more guns, more guards, but, in fact, to make sure that the personnel at the laboratory have training to know what information they can talk about, when its sensitive, when it needs to reported, who it needs to be reported to. I'm not sure that following this hearing, or following the GAO report, or following the letter the Secretary, that I'm comfortable—I'm not speaking for the subcommittee—that I'm necessarily comfortable to know that we're all aimed in that direction. That we train all of these people at the laboratories to know what methodologies may be used against them to gain this information that they, in fact, receive the best training possible. So, I think that we've got a lot of work cut out to make sure that we're able to oversee this.

Mr. UPTON. We do have a lot of work to do, and I guess, Mr. Stupak, did you have another question or two?

Mr. STUPAK. I just would like to ask one. The last questions were whether Los Alamos was marginal or excellent based on the evaluations. Now, Secretary Richardson, has changed the reporting structure, so that the offices of intelligence and counterintelligence report directly to the Under Secretary. The independent evaluator of these programs, and others in safeguards and security, are still lower level, if you will, or down in the bowels in the Environment, Health, and Safety division. So, if they're way down there, who's really going to tell the Secretary, the Under Secretary, National Security Council, or President that things aren't going well?

Mr. REZENDES. The way the structure is, they are.

Mr. STUPAK. Who is they?

Mr. REZENDES. The Office of Security and Evaluation, which is within the Assistant Secretary of Environmental Health and Safety.

Mr. STUPAK. So, you're confident that accountability and responsibility is going to be carried out?

Mr. REZENDES. No. My confidence level wasn't there. In fact, we think that they are independent. I think how they performed recently and historically in terms of the kinds of evaluations they do, are pretty straight. But, I'm not sure what kind of information the Secretary is getting from those evaluations, or the kinds of priority attention in terms of how it translates into the budget, not only

from headquarters, but also within these facilities to make sure that those things are corrected.

Mr. KLINK. Would the gentleman yield? I think that what he gets to, Mr. Rezendes, is the point that we were making earlier on, and that is this has not been a priority.

Mr. REZENDES. Correct.

Mr. KLINK. Is it now a priority? Are we heading toward making it a priority? Can you help us——

Mr. REZENDES. Yes. In fact, I've talked to Ernie Moniz, who is the Under Secretary, and he is heading up at the Secretary's request, a reorganization to look at the very security elements at headquarters, and how they report the lines of authority and responsibility there, which we think is really vital to making sure that some of this stuff is going to work. But even squaring that away, you still have DOE as an agency that is essentially run by contractors throughout the United States. That has to cascade down into a responsibility and accountability with contractors. Put it in the contract hold them accountable for making sure that they're doing what they're supposed to do. Also, hold the Federal employees that oversee these contractors accountable to make that they ensure that the contractor does what he's supposed to do.

Mr. STUPAK. Well, if they're still in the Environment, Safety, and Health divisions, how do you make sure these people who are going to do these reports remain independent of DOE, and that direct line is accessible and available to them when things go wrong?

Mr. REZENDES. Well, particularly, what kind of information is being filtered to the Secretary, and also, what kind of priority and oversight is he providing to the contractors to make sure that things happen.

Mr. STUPAK. Thanks. Nothing further. Thank you, Mr. Chairman.

Mr. UPTON. Mr. Rezendes, we appreciate very much your time this afternoon. We appreciate your report. This is the first time that I've chaired a subcommittee that has had you come before us, and we appreciate your time on this, and giving us the report, and your testimony today. We clearly have a lot of work to do. You've helped guide, I think, in the process as we begin this quest. In going through your report, literally page by page, we look forward to implementing all of the recommendations that you had. We look forward to working with the Secretary of Energy to make sure they do, in fact, take place. Thanks very much.

Mr. REZENDES. Thank you.

Mr. UPTON. This hearing is adjourned.

[Whereupon, at 4:07 p.m., the subcommittee was adjourned.]