WEAKNESSES IN CLASSIFIED INFORMATION SECURITY CONTROLS AT DOE'S NUCLEAR WEAPON LABORATORIES

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JULY 11, 2000

Serial No. 106–148

Printed for the use of the Committee on Commerce

(

U.S. GOVERNMENT PRINTING OFFICE
67–110CC WASHINGTON : 2000

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

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

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM 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:	
Aftergood, Steven, Senior Research Analyst, Federation of American Scientists	169
Browne, John C., Director, Los Alamos National Laboratory	152
Glauthier, T.J., Deputy Secretary; accompanied by: General Eugene E. Habiger, Director, Office of Security and Emergency Operations; General John McBroom, Director, Office of Emergency Operations; and General Tom Gioconda, Deputy Administrator for Defense Programs, National Nuclear Security Administration, Department of Energy	140
Podonsky, Glenn S., Director, Office of Independent Oversight and Performance Assurance, U.S. Department of Energy	16
Robinson, C. Paul, President and Laboratories Director, Sandia National Laboratories	145
Tarter, C. Bruce, Director, Lawrence Livermore National Laboratory	164
Wells, Jim, Issue Area Director, Energy, Resources, and Sciences Issues, U.S. General Accounting Office, accompanied by William F. Fenzel	11
Material submitted for the record by:	
Aftergood, Steven, Senior Research Analyst, Federation of American Scientists, letter dated August 1, 2000, to Hon. Fred Upton, enclosing response for the record	215
General Accounting Office, response for the record	218
Robinson, C. Paul, President and Laboratories Director, Sandia National Laboratories, responses for the record	216

WEAKNESSES IN CLASSIFIED INFORMATION SECURITY CONTROLS AT DOE'S NUCLEAR WEAPON LABORATORIES

TUESDAY, JULY 11, 2000

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

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2322, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Cox, Burr, Bilbray, Ganske, Bryant, Stupak, Green, and DeGette.

Also present: Representative Wilson.

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

Mr. UPTON. Good morning, everyone. Today we will continue this subcommittee's focus on the security problems apparently still unresolved at DOE's nuclear weapon labs, as evidenced by the most recent security breach at Los Alamos involving some of the Nation's most sensitive nuclear weapons-related data. This data, containing hard drives utilized by DOE's Nuclear Emergency Search Team, or NEST, includes information on detection of and response to incidents involving improvised nuclear devices or other nuclear weapons in the United States or foreign stockpiles.

Many of the shocking facts concerning this latest incident already have made their way into the public. We all know about how 26 individuals had unrestricted access to the vault containing these sensitive NEST hard drives and that they could take them at any time without creating any written record of their removal.

But recent committee staff interviews of relevant Los Alamos officials have revealed that roughly half of these 26 people, including the vault custodian, were not members of the NEST team and did not have any, "need to know" the information contained on those hard drives.

Thus, numerous individuals, without any legitimate reason to have access to this highly sensitive data, could have entered this vault at virtually any time and taken these hard drives without anyone knowing. Instead of "need to know," we had a system of "want to know."

We also have recently learned that Los Alamos failed to change the combination on the vault as required when there are changes to the authorization access list. In fact, the last time the vault com-

bination had been changed was in 1996, despite changes in the list of authorized personnel since that time.

Thus, individuals beyond those 26 whose involvement in these programs had already ended continued to have access or could have continued to have access to the vault.

These particular deficiencies reflect poorly on Los Alamos, and there is no doubt that there was substantial confusion at the lab about who was supposed to be doing what when it came to security of classified assets used by NEST.

Part of this confusion stems from the fact that line managers believed the lab program officials were in charge, while the program officials thought the opposite. But part of this confusion also arises from the unique situation of these DOE-led swat teams like NEST. We have learned that DOE headquarters essentially picked the NEST management team at Los Alamos, which in effect reports to DOE on operational issues, while reporting through the lab management structure on administrative issues.While this arrangement probably makes sense, it requires close coordination and communication to make it work, and we now know the price of such failure.

The greater problem, however, goes beyond this particular team to the overall system in which it operates. As our first panel today will explain, DOE essentially has set a low threshold of security requirements for its labs to follow, leaving them substantial discretion and flexibility on how they implement actual security practices.

The result—as both Mr. Podonsky's and this committee's oversight have discovered—is that the effectiveness of security practices at the labs varies greatly, both within and among the labs, even for very similar types of information. And because of the lack of clear and tough requirements, the built-in system of laboratory and DOE security oversight is destined to failure, since virtually any state of affairs could be considered to be technically in compliance with DOE orders. Thus, while DOE may want to blame the labs whenever something goes wrong in security, it seems clear that the real fault lies much closer to home.

The saddest fact is that the most recent national security threat posed by these missing hard drives might have been avoided had numerous expert recommendations to the administration been implemented in a more timely fashion.

As far back as 1994, DOE and the Department of Defense were engaged in discussions to increase controls on the more sensitive nuclear weapons information that the two agencies share, such as the data on these hard drives, but no consensus was ever reached. In February 1996, a draft report commissioned by Secretary of Energy O'Leary recommended that higher security fences be established for similar categories of data, but DOE failed to issue a formal proposal to DOD until December of last year, and it seems that Defense will not lightly accept such recommendations anyway, for its own reasons.

And two 1999 recommendations, one from the labs themselves and another from the President's Foreign Intelligence Advisory Board, urged DOE to tighten control requirements for such data, apparently to no avail. Nothing prevented DOE from tightening

controls on its own material while in its possession, even if DOD opted not to go along. Indeed, it is now doing so in response to the latest crisis.

Yet instead of tightening controls on our most sensitive secrets years ago, DOE moved in the exact opposite direction. In January 1998, DOE eliminated controls on Top Secret data, much as DOE had reduced controls on lower level classified matter back in 1992.

Today's hearing hopefully will allow us to have an honest discussion of what is and what is not required by DOE orders and what is and what is not being done by the labs to properly control access to our Nation's most sensitive nuclear information, and what more should be done to remedy this situation.

I echo Chairman Bliley's call today for a more centralized Federal role in security affairs at our nuclear weapons labs. Let's leave the science to the scientists, but let's make security the responsibility of Federal security experts over whom we have direct and personal accountability.

I yield to the acting ranking member of this subcommittee, from the great State of Michigan, Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman, and thank you for holding this hearing. Last time this subcommittee had the opportunity to ask questions about the missing hard drives at the Los Alamos National Lab, the Department of Energy witnesses had few answers to give this subcommittee. Today we know the hard drives have been found. Although the investigation is not complete, the FBI and the DOE do not believe the missing hard drives were the result of espionage. Rather, their loss resulted from sloppy handling and potentially criminal attempt to cover up the cause of their loss.

The chain of events that led to the discovery of the missing hard drives has been well publicized. The Los Alamos lab took 3 weeks to inform the DOE of the missing hard drives when it was required to do so within 8 hours. The procedures at Los Alamos for handling the secret nuclear weapons information was completely inappropriate.

While all three of the labs have inadequate procedures for handling this material in place, Los Alamos allowed more people greater access with fewer controls than either Sandia or Livermore.

You know, Mr. Chairman, the McDonald's restaurant employees check the cleanliness of their bathrooms and keep better records of their maintenance than Los Alamos does of its nuclear weapons data. As a result of the loss of these drives, I and other members of this subcommittee wrote Secretary Richardson asking him to terminate the contract with the University of California, because it has been unable to perform its security functions in accordance with its contract with the Department of Energy and its responsibility to the American people.

Time and time again, the labs have asked us to excuse their mistakes, overlook their failures and trust them to properly handle sensitive materials they are entrusted with. I don't know about you, Mr. Chairman, but I am all out of trust.

Although I was a State police officer for many years, I am certainly not a nuclear security expert. Yet, when I analyzed the proposed improvements to the proposed tracking and inventory proce-

dures at Los Alamos, I am left scratching my head. Los Alamos will institute a new bar coding system that will allow these sensitive documents to be inventoried, but it will not allow the lab to track who has the information. What is the use of bar coding the information if you can't track who is removing it and who has it?

As I mentioned in the earlier testimony and before this last subcommittee meeting, the Menominee Public Library has the ability to use its bar coding system to make sure when a book leaves the library. The coding system will also tell you who has the book, who removed the book. Why can't Los Alamos do the same? I am starting to believe that DOE should award the contract to Menominee Public Library.

Mr. Chairman, I don't believe the labs have produced any evidence to assure me that they are suddenly going to take their security function seriously. Rather than complain about budget cuts or other concerns, the labs need to require their people to do their job and protect our Nation's nuclear weapons data. McDonald's and the library keep track of their employees and property for a lot less than Los Alamos. I believe it is time for common sense and action, not more excuses.

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

Mr. UPTON. Thank you.

Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman.

Once again, this subcommittee is meeting to examine security problems at the Department of Energy in our Nation's nuclear weapon laboratories. Needless to say, I am disappointed to be here. I had hoped that the work of this subcommittee, the Cox Commission, the President's Foreign Intelligence Advisory Board, and others over the course of the last year would have prompted DOE to take action. Unfortunately, that's not the case.

While Secretary Richardson has taken some steps to improve physical security at the labs, it appears as though DOE has ignored, until recently, recommendations suggesting basic changes in the way the agency does business.

Once again, we are forced to bring the Department and the labs to Congress to figure out why these incidents continue to occur. No one is suggesting that we will be able to prevent all security lapses or stop every spy, but we can certainly take steps to make it as difficult as possible for them to occur in the first place.

Over the last year, a number of recommendations have been made and a number of recommendations have been ignored. Last summer, for example, Senator Rudman made some very specific recommendations: establish clear chains of authority; implement effective personnel security programs; reinstitute comprehensive classified document control systems; and conduct a comprehensive classification review.

Once again, recommendations made and recommendations apparently and unfortunately ignored.

We know they were ignored because Mr. Podonsky's recent review of Lawrence Livermore and Sandia contained similar recommendations. Secretary Richardson has apparently determined that responsibility for security belongs with the labs. If it were only that simple.

I have been among the most critical of the labs' management practices, but it is clear that Secretary Richardson's arguments ring hollow. The Department has a responsibility to see that its security policies are clear and leave no room for confusion. Its policies are anything but clear and confusion reigns.

The Podonsky review indicates that the labs have generally implemented standard DOE policy. The labs do indeed bear some responsibility for security failures that occur on their watch, but clearly the policies in place at DOE deserve equal attention. Despite Secretary Richardson's protest to the contrary, there is simply no clear guidance from DOE on security issues, period.

Nowhere is that lack of guidance more readily apparent that than in the NEST program. This little known element of DOE is one of the most important tools in our national security apparatus. The lack of accountability and absence of clear lines of authority in this program are extremely disturbing. The lab directors and DOE managers seem to be consistently at odds over who is responsible for the program. This program is too important for disputes over who is accountable. Someone is. And this member, for one, intends to find out who.

I also have to express my disappointment with General Habiger, General McBroom, and General Gioconda. Gentlemen, I have the utmost respect for the long years of service and sacrifice you have given to your country. Perhaps better than any others, you understand the threats posed to our Nation by nuclear weapons and the damage that could be caused to our national security should such sensitive information fall into the wrong hands. That's why we ask you to continue your service to your Nation at the Department of Energy. We hope that your backgrounds and knowledge of security issues will serve to strengthen what has historically been weak security programs.

Somehow, some way, you have lost that focus. Perhaps the culture of disregard for security at DOE is actually so pervasive that it consumes all who attempt to run, but we expect you to fight against that culture. You are all take-action types. But why haven't we? When you recognize a problem, you should take the steps to correct it. That's how you became generals in the first place. You were brought in to DOE to continue that approach and to pass on your security-conscience attitudes to the rest of that Department. Gentlemen, we expect a great deal from you. We want you to succeed. The Department has a long way to go to improve its security programs and we will continue to turn to you for the answers.

This member, and I expect this entire subcommittee, stands ready and able to do whatever the request is.

With that, I yield back, Mr. Chairman.

Mr. UPTON. Thank you. Mr. Bilbray.

Mr. BILBRAY. Yes, Mr. Chairman. Mr. Chairman, I would like to echo my colleague from Michigan, the acting ranking member, and I want to—mostly because he is here—I want to praise him—or because he is not here, I want to praise him. The fact is is that I think that he articulated the issue that this is not a partisan issue, it is an American issue. I for one am very, very concerned that we handle this in a very nonpartisan way. I want to ask my colleagues on the Republican side to remember that the implementation of

whatever correction we have will probably be executed by another administration in another year, and sadly looking at the next—until the end of the year, of basically just trying to cover ourselves until that set time.

I also want to point out to my Democratic colleagues that defending a status quo, either be it from a previous administration or this administration, doesn't solve the problem and doesn't avoid future risks.

Mr. Chairman, the 7-Eleven stores in America can tell you who picked up lip balm at their counter 3 months ago. They can give you that type of inventory control because they use very simple technologies: time delayed video surveillance.

There is almost no company in America that I know of, and especially in my district with all the high-tech work, that do not have what appears to be a much superior security, not just system but mindset, than what we have seen to have been exposed with our laboratories.

Now, Mr. Chairman, I want to say that I don't know, speaking to generals, about what is going on in the Army or the Air Force, but as somebody who worked around nuclear facilities and nuclear crafts in the United States Navy as a contract worker, I know the security that the United States Navy puts to its nuclear secrets and its nuclear information. And as a worker, firsthand exposure to this, I tell you I am almost to the point of saying, why can the United States Navy be able to secure its secrets and its information about its ships that are sitting in the middle of a 2 million population and all at once watch our laboratories misplace information that's as critical as we have seen in the last year?

I just think that we have got to recognize, though, that it is not just the systems's breakdown that we have witnessed in the last few years, and I would ask my colleagues and the witnesses to address the issue of the mindset that has infected this agency, the mindset which appears to be that this is a campus environment that is not the precious treasure of information that is owned by the people of the United States, and only the people of the United States. It is not the personal property of the laboratory, of the university system, or of the world. It is the taxpayers of the United States who developed this information. It is their right and their right only to be able to use it as they see fit.

Mr. Chairman, I appreciate the chance to be here today. I think this is a very important challenge, and I think it is a challenge to all of us in Congress to be able to understand that we need to find answers and we need to implement responses. If my 15- and 14-year-old children had lost their disks and said, "Well, we are lucky, dad, nobody stole them, I just misplaced them," as a parent I would be more outraged at the fact that my children did not take care of what was their responsibility, even more than thinking that they allowed somebody to steal it.

I don't think we should celebrate the fact that they were lost. I think that we should be frustrated and terrified that they were lost. And I yield back, Mr. Chairman.

Mr. UPTON. Thank you. Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I am glad to follow my San Diego colleague, and I agree that this is a bipartisan issue and

it is a national security concern that should be bipartisan or nonpartisan. I know not only do we need these continued hearings, but we need to follow up with the appropriations necessary with the Department of Energy. And also as testimony in our earlier hearings showed, we need to follow up to make sure the money is spent for the security issues.

Like all the members of the committee, and I think all of Congress, we have become increasingly concerned about security controls at DOE and the weapons—nuclear weapon laboratories and the disappearance and the reappearance of the sensitive hard drives, and I believe improvements are necessary. And whether it is changing the contract or maybe bringing someone else in to make sure, I know we benefit from the campus-like attitude that we have at both Los Alamos and the other facility, but we also need to make sure that that campus-like attitude is not to the detriment of the national security of our Nation.

I know it is a concern we have, but the testimony we have had for a number of hearings is that this is not a current problem. Sure, we have it now and we hear the problems, but it is a recurring problem over the last number of years and in different administrations. So I don't want it to be just a Secretary Richardson problem. It is a national problem that spans both Republican and Democrat, but we need to solve it.

That's why, Mr. Chairman, I thank you for having these hearings and to keep the follow-up. We need to make sure that we don't have these hearings a year and a half from now and find out something else was misplaced, whether it is the easiest thing of putting security cameras in sensitive areas, but again there are lots of solutions that could be done and hopefully DOE and the administration will do it on their watch and not wait until the next watch.

Thank you, Mr. Chairman.

Mr. UPTON. Thank you. Dr. Ganske.

Mr. GANSKE. Mr. Chairman, in March 1999, following the Cox Commission report findings, the three lab directors wrote to the DOE Under Secretary, urging that formal accountability requirements for Secret and Top Secret restricted weapons data be reinstituted, "as quickly as possible." The Redmond report, issued shortly thereafter, contained a similar recommendation, but DOE did not take any apparent action to address these recommendations prior to this latest security incident.

A couple of weeks ago this committee meet in secret, received a briefing on this problem, and what I will say—it has been reported in the press—and that is that the information on those disk drives were pretty important. I was astounded at that briefing at the lack of commonsense security arrangements, to say the least.

So I think there are some things that we need to determine in this hearing. For instance, why does there seem to be such a big difference between DOE minimum security requirements and commonsense security controls, as outlined so well by Mr. Stupak already?

Why has DOE failed, since 1996, to act on repeated recommendations to impose tighter controls on its most sensitive nuclear weapons information? And why did DOE in 1998 actually move in the other direction by eliminating controls for Top Secret data? Those

are all very important questions for us to determine today in this hearing. And I thank you, Mr. Chairman, for calling this hearing.

Mr. UPTON. Thank you. I would just note for the record that for those members that are not here, we will leave the record open for opening statements and I would make a unanimous consent request that all members of this subcommittee will have an opportunity to submit their opening statements as part of the record. Without objection.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. ED BRYANT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Thank you Mr. Chairman: I appreciate your holding this very timely hearing, and I want to welcome our distinguished panels.

In May of last year, the nation was shocked to learn that a suspected Chinese spy had been repeatedly transferring top-secret computer files at the Los Alamos National Laboratory from a classified system for over 10 years before he was finally arrested. These computer files contained classified programs used to develop, build, test and simulate several generations of nuclear weapons. According to the Los Angeles Times, the loss of this information represents ''a staggering blow to U.S. national security.''

A little over a month after learning of this security breach, the full Commerce Committee held a hearing on Department of Energy security lapses. During this hearing, the chairman of the President's Foreign Intelligence Advisory Board, former Senator Warren Rudman, reported that his commission had found evidence of serious security failings, including: foreign scientists visiting labs without proper background checks and monitoring; classified computer systems and networks with innumerable vulnerabilities; and instances where secure areas were left unsecured for years.

In the wake of this report, Secretary of Energy Bill Richardson stated that ''I can assure the American people that the nuclear secrets are now safe.'' Less than a year later, however, news agencies began reporting that two computer hard drives containing sensitive information about U.S., Russian, and other nuclear weapons was missing. The information on these disks is used by the Nuclear Emergency Safety Team (NEST) to respond to terrorist activities or accidents involving nuclear weapons.

Investigations into the disappearance of these hard drives have revealed that security was so lapse that the 26 NEST members were able to enter the vault where these devices were stored without ever having to sign in or sign out. NEST team members were also able to remove and return sensitive nuclear information without filing any type of report.

Although the hard drives were recovered a few weeks ago, during a recent Senate hearing it was revealed that the information on these drives could have been copied in such a way that we may never know if this information has been given to other countries.

The Department of Energy has just recently announced plans to tighten security by replacing combination locks with more sophisticated palm scanning locks, and possibly installing video surveillance systems. While this is encouraging, it is a little like closing the barn door after the horses have decided to leave. The real question, isn't what can the Department do to tighten security, but why wasn't this done before our nation's nuclear secrets were compromised.

I look forward to hearing today's testimony but I want the folks from DOE to listen carefully. I do not want to hear what has become a seemingly boiler plate answer that ''yes, mistakes were made and we are fixing the problems.'' I have heard that too many times before and without fail another security breech has closely followed such supposedly reassuring statements. I believe it is time for a more frank discussion, I'm owed it, this Committee is owed it and most importantly, the American people are owed it.

I thank the chair and yield back the balance of my time.

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

Thank you, Mr. Chairman. Today we continue our long-running effort to get to the bottom of DOE's security problems. The latest incident involving the disappear-

ance, and now mysterious re-appearance, of two highly sensitive hard drives used by Los Alamos's nuclear emergency search team has already been the subject of numerous press reports and Congressional hearings, including one by this Subcommittee several weeks ago when the story first broke. But today's hearing will go beyond this single incident, to expose a security system that has deep flaws—a system that has failed to keep up with the changing security threats we face, and the ability of technology to both hurt and help our security posture.

Based on the Committee's oversight work in this area, last Fall I became increasingly concerned about how DOE and its labs were controlling access to their highly sensitive information, such as that found on these missing hard drives. I instructed Committee staff to work with the General Accounting Office to set up a review, and we reached agreement on a scope of work in March of this year. Little did we know, at that time, how timely this work would become.

GAO is with us today to lay out its findings from the first portion of its review—a survey of what DOE does, and quite surprisingly does not, actually require of its labs when it comes to controlling classified data, and how these requirements have been weakened over time. While DOE's requirements don't tell the whole story—the labs often do more than is required—they are, nonetheless, an important part of why we're in the trouble we're in today. As DOE's own internal inspectors will tell us today, DOE's minimal, and terribly vague, security orders create a situation in which inconsistency and ineffectiveness can, and often do, reign supreme.

Indeed, what both of these recent GAO and DOE independent reviews confirm is something that this Committee has been exposing for years—that the labs can be in total compliance with DOE security requirements and still have poor security practices. And we don't have to look any further than the latest Los Alamos security breach for an example. Yes, it appears that Los Alamos violated at least some DOE requirements, and swift punishment should follow. But the facts that have most of Congress and the American public up in arms—the lack of any record of who enters these sensitive vaults and removes classified data—do not amount to violations of DOE orders. In fact, as GAO and DOE experts will tell us today, the Department does not now have, and never has had, such specific requirements for even highly sensitive data. The suggestion by some that changes in controls in the early 1990s did away with such common-sense requirements is thus simply not true, and should not be used as an excuse for the pitiful current state of affairs.

Los Alamos and the other nuclear weapon labs certainly can be faulted for following such minimal requirements and not using better local judgment in protecting highly sensitive assets. But it also must be noted that, in many cases—particularly at Sandia—the labs imposed greater controls than required by DOE, and fought efforts by DOE Headquarters to weaken them. And when the Cox Commission raised concerns last Spring about Chinese espionage at the labs, the lab directors urged DOE to tighten requirements for control of nuclear weapons data "as quickly as possible"—a recommendation that either fell on deaf ears or through the bureaucratic cracks, as similar expert recommendations had since 1996.

I firmly believe that, at the end of the day, responsibility for setting and enforcing proper security controls on this Nation's most sensitive nuclear secrets must be borne by the Federal government. The current system—which allows DOE to blame its contractors, and its contractors to return the favor—will never truly achieve effective security. The new National Nuclear Security Administration, designed by Congress to streamline the chain of command and enhance accountability for security, so far has done neither. Despite a proliferation of "generals" within DOE—as evidenced by our witnesses today—we don't have any greater accountability. Indeed, all of these generals will tell us that they didn't know about, and weren't responsible for, the poor state of security affairs at Los Alamos with respect to these missing hard drives, and similarly sensitive materials scattered throughout these weapon labs.

We need to put this nuclear agency's security chief firmly in charge of *both* security policies *and* practices at our weapons labs—and hold him personally accountable for future failures. And the days of relying on Federal contractors to establish security practices must end.

Finally, let me urge caution against any reactive effort by either DOE or the Congress to try to impose a one-size-fits all approach to information security at DOE, or to return to out-dated notions of information "accountability." As we will see today, the pre-1992 controls, if they had been left in place, would not have prevented this latest incident at Los Alamos, nor would they have made our job of detection and investigation significantly easier. Manual, paperwork-intensive controls do little to catch those intent on avoiding them.

So the answer is not to return to the old rules, but to develop new ones that take into account the different risks that increases in technology and the use of electronic

media pose to our nuclear security. At the same time, we also must embrace the benefits of today's technology, which allows us to better control and track our most sensitive data in a more effective and less costly manner—technology being used today by private industries ranging from high-tech powerhouses to our local grocery stores. While these technologies surely are not the theft-proof panacea some might suggest, they do provide a good starting point. I look forward to this debate, and thank you Mr. Chairman for holding today's hearing.

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

Thank you Mr. Chairman.

I plan to make my remarks brief so that we may more quickly hear from our witnesses.

I would like to thank our witnesses for coming today, I look forward to hearing from you. Unfortunately, I have another hearing that conflicts with this one so I will probably have to step out from time to time.

As you know, we had a rather timely hearing on this subject roughly a month ago, just a day after it was revealed that computer hard drives containing sensitive nuclear defense information were missing from Los Alamos National Laboratory. I know that some of our witnesses, along with Secretary Richardson, have been working hard over the past month to ensure we know what happened to the material these disks contained, and to ensure that this kind of inexcusable security lapse does not happen again in the future. I recognize that you may not have much new information, or at least information appropriate for an open hearing, but I do look forward to an update on the progress of the investigation.

On June 15, 2000, I joined five of my colleagues in sending a letter to Secretary Richardson. Our letter requested that the Secretary revoke the University of California's contract to manage and operate Los Alamos National Laboratory because repeated security violations represent a breach of contract. We obviously did not make this request lightly. We all recognize the tremendous intellectual value the University brings to our national defense and research programs. The problem is that the University does not seem to be able to effectively manage the contract, which directs them to provide security and comply with Department of Energy security rules and procedures. The University has an outstanding reputation and has great intellectual assets, this does not mean it has the capacity to operate an effective security program.

I do not hold the University singularly responsible. The Department of Energy bears some blame. It is the Department's responsibility to oversee the contract and provide that proper security guidance, rules, and enforcement authority exists. It certainly appears that the Department has never mastered these functions. We should all agree that this is not a partisan issue. These problems go back years through both Democratic and Republican Administrations.

I understand that the Department is now considering issuing a security contract. Unfortunately, adding yet another contractor into the mix is not likely to solve the problems we are here to discuss today. I am not very confident that a new contractor whose role may be relegated to providing technical assistance on security matters to laboratory management is going to remedy our security problems.

I thank you Mr. Chairman for calling this hearing.

I yield back the balance of my time.

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

Thank you, Mr. Chairman for holding this hearing, and for the bipartisan staff work that led up to it. Security at DOE weapons laboratories is a longstanding and stubborn problem. For example, last year, after the downloading of nuclear weapons information by a weapons scientist from classified computers at the Los Alamos National Laboratory, the Rudman panel concluded that the Department of Energy "and the weapons laboratories have a deeply rooted culture of low regard for and, at time, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO [General Accounting Office] and the House Energy and Commerce Committee."

But even the recommended changes in structure—even if fully implemented could not guarantee security. According to Senator Rudman, "[T]he most powerful guarantor of security at the nation's weapons laboratories will not be laws, regulations, or management charts. *It will be the attitudes and behavior of the men and women*

who are responsible for the operation of the labs every day." Those attitudes ranged, according to the panel, from "half-hearted, grudging accommodation" to "smug disregard."

Secretary Richardson took many steps to correct deficiencies. Most significantly, the Department hardened its security and greatly expanded the counter-intelligence operation. I wish that I could say the same about the laboratories. Upon the order of Secretary Richardson, the laboratories had a two-day security training stand-down last year, but apparently it was not sufficient to change the culture.

In many ways, the loss of the hard drives at Los Alamos reflected that ingrained culture even more than the Wen Ho Lee incident did. It involved not one person, but many who knew that they were violating DOE's security directives when they did not report the missing disks. Someone—deliberately or otherwise—removed the hard drives from their secure location. Many, many other people tried to cover up the loss. But why shouldn't they? No one was disciplined for the weak cyber security last year. Why would anyone be punished now?

The University of California will tell us today of its "integrated security and safeguards management" system which will instill security awareness in every employee. Perhaps it would have prevented the latest incident. But it is still not operational. Mr. Chairman, the chronic security problems at Los Alamos led me and five other Democrats on this Committee last month to call for the removal of the University of California as the contractor at Los Alamos. Only when contractors understand that there are real consequences to pay for security breaches will they make necessary changes.

Mr. UPTON. This morning, for our first panel, we have Mr. Jim Wells, Issue Area Director for Energy Resources and Science Issues of the U.S. General Accounting Office. Welcome, and you will be accompanied by Mr. Fenzel.

We also have Mr. Glenn Podonsky, a familiar face to members of this subcommittee, Director of the Office of Independent Oversight and Performance Assurance at the Department of Energy.

As you gentlemen know, we have had a longstanding tradition of taking testimony under oath. Do you have any objection to that?

Mr. PODONSKY. No.

Mr. WELLS. No.

Mr. FENZEL. No.

Mr. UPTON. The committee rules also allow you to have counsel help represent you. Do you wish to have counsel?

Mr. PODONSKY. No.

Mr. WELLS. No.

Mr. FENZEL. No.

Mr. UPTON. If you would stand and raise your right hand.

[Witnesses sworn.]

Mr. UPTON. Thank you. You are now under oath.

Mr. Wells, we will start with you and I would note we would like you to keep your remarks to about 5 minutes and your entire statement is now part of the record. Mr. Wells.

TESTIMONY OF JIM WELLS, ISSUE AREA DIRECTOR, ENERGY, RESOURCES, AND SCIENCES ISSUES, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY WILLIAM F. FENZEL; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE, U.S. DEPARTMENT OF ENERGY

Mr. WELLS. Thank you, Mr. Chairman, members of the subcommittee. Once again, GAO is here to present information——

Mr. UPTON. If you would just pull the mike just a little closer so the folks in the back can hear.

Terrific. Thank you.

Mr. WELLS. Once again, GAO is here to present information regarding a lapse in security at the Department of Energy. Accompanying me today is William Farrell Fenzel, our assistant director, who over the years has done a lot of the security work in the Department of Energy.

At your request several weeks ago, we received a letter asking for an audit investigation of accountability of classified material controls that were in existence at the Department of Energy. That audit has begun and it is still ongoing.

During our work, you asked us today to appear before this committee to discuss the answers to two questions. The first question was, what are the minimum DOE requirements imposed on classified material by the contractors who do the work for the Department of Energy? And the second question was, are document sign-in and sign-out sheets required?

We have this information. It is shown in pages 4 and 5 of my written statement, but I will also refer to the charts on my left-hand side. What I would like to do is quickly just highlight those charts that deal with Secret and Top Secret requirements to show you how basic accountability requirements have changed over the last 12 years.

I want to turn your attention now to the Secret chart. These are changes in the minimum requirements for controlling secret documents.

What you see on the left-hand side are typical accountability document requirements, things like frequency of inventories. These are the types of things that were required under DOE, things like unique identification numbers, putting a number on a document so that you know whether that document is present or not; things like approval for reproduction so before one can make a copy of a classified document, one must go back to the originator of the document, and seek permission and document that an extra copy has been made. As you can see by that chart, most of those requirements were dropped and discontinued in 1992.

If I could refer you to the second chart, which talks about some of the changes in the minimum requirements for controlling Top Secret documents, once again on the left-hand side you will see typical accountability-type controls. What I would like to point out for Top Secret documents, in terms of DOE minimum requirements, is that some of these requirements have been reduced not once but twice.

Looking at frequency of inventories, as you can see, required every 6 months in 1988. That was changed to annually in 1995, and in 1998 the requirement for inventories was discontinued.

Looking at items like a Top Secret control officer and end-of-day verification, we are talking about a requirement that did exist at one time for a custodian, a person that would know who had what document and where, and at the end of each day would verify and certify that the Department of Energy had control over where that particular document was.

And last, let me answer that question in terms of whether there are required sign-in and sign-out sheets. Based on our audit team's discussion with agency officials, we have spent hours combing hundreds of pages of DOE orders and current security manuals and

cannot find any requirement, minimum requirement, for sign-in and sign-out sheets.

The bottom line, Mr. Chairman, clearly what you see represented on those charts document that the requirements have gone down, or as Mr. Bilbray talked about, the threshold has been lowered.

This is what we found to date. We still need to look at what is being done in terms of the actual practices; even why these changes are being made and what impacts, if any, exist out there when we finish our audit for this committee.

Mr. Chairman, I am going to stop here. I probably have a couple more minutes but I am going to stop here because I think we have much more to do and a lot more answers to come up with. We do, however, share the concern of the committee about document accountability and, like you, we too look forward to hearing the answers of the witnesses that follow this panel.

Mr. Chairman, thank you. We will be glad to respond to any questions you may have.

[The prepared statement of Jim Wells follows:]

PREPARED STATEMENT OF JIM WELLS, DIRECTOR, ENERGY, RESOURCES, AND SCIENCE ISSUES, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION, GAO

Mr. Chairman and Members of the Subcommittee: We are pleased to be here today to provide information on the Department of Energy's (DOE) requirements for protecting and controlling classified documents. DOE's requirements are designed to protect classified documents from their inception to their destruction. At the Subcommittee's request, we have begun an evaluation, which is still underway, of DOE's classified matter protection and control program. During the past few weeks, we briefed your staff on DOE's requirements for controlling classified documents. At your request, we are testifying today on changes in DOE's requirements since 1988, when complete accountability was required for Secret and Top Secret documents. You also asked us to testify on the extent to which sign-out sheets have been required to provide a record of who removed a classified document from storage and when it was removed.

I would like to emphasize that the requirements we address today are DOE's minimum requirements. The contractors who operate DOE's facilities may require additional controls and procedures to protect and control classified documents. We are providing information on the requirements for controlling both Secret and Top Secret documents in protected areas. Protected areas have physical barriers and also have controlled access. Secret and Top Secret documents stored outside of these areas require additional protective measures.

In summary, DOE has numerous procedures designed to protect classified documents. The requirements vary depending on the type of document being protected and the nature of the protection provided where the document is stored. We found that many requirements for protecting and controlling Secret and Top Secret documents stored in protected areas were discontinued in the 1990s. For example, the requirement to inventory Secret documents every 3 years was discontinued in 1992 with other controls over Secret documents. In regard to Top Secret documents, many requirements, such as a Top Secret Control Officer, were eliminated in 1998.

Background

DOE is responsible for administering a security program that protects classified documents from loss or theft. DOE's memoranda, orders, and manuals set forth the requirements for protecting and controlling classified documents at DOE facilities. DOE's strategy for protecting classified documents involves a "graded protection" system. Under such a system, the level of protection for a classified document is commensurate with the threat to the document, the vulnerability of the document, the value of the document, and the level of risk to the document that DOE is willing to accept. Not all items are protected to the same degree; furthermore, locations on a DOE site may be protected differently. Protection is provided by various means, such as physically protecting classified documents with guards, buildings, vaults, and locks; limiting access to classified documents to personnel with proper security clearances and a legitimate need to have the information; and the processes and procedures known as classified matter protection and control.

DOE's classified matter protection and control program has included a wide variety of requirements. These requirements have included conducting inventories of classified documents and maintaining an accountability record for each classified document. The accountability record can include a description of the document, date, classification level and category. DOE has also required that each classified document be assigned a unique identification number—to allow the identification and tracking of the document—and a copy and series designation—to provide information on how many copies exist. Additionally, DOE has required the use of receipts for internal and external distribution to provide a record of dissemination of a classified document within a facility and outside a facility, respectively. Finally, DOE has required certain procedures for maintaining receipts and destruction records and obtaining approval for the reproduction of a classified document. Other requirements could also be used, such as maintaining a sign-out sheet to provide a record of who removed a classified document from storage and when it was removed.

DOE has also required additional controls for Top Secret documents. These have included assigning a Top Secret Control Officer, who has ultimate responsibility for Top Secret documents; conducting a verification to certify that all Top Secret documents have been returned to storage at the end of each work day; and maintaining a Top Secret access record that lists all persons who are authorized access to Top Secret documents.

Changes to DOE's Requirements Over the Past 12 Years

In general, over the past 12 years, many requirements for Secret and Top Secret classified matter protection and control have been discontinued. Specifically, requirements for maintaining records and receipting and reproducing classified documents were discontinued. According to DOE classified matter protection and control officials, these changes were implemented to promote governmentwide uniformity among contractors and to account for technological changes, such as computers, copiers, and faxes, in the processing and storage of classified information. In our ongoing evaluation, we will be looking at how other agencies protect and control classified documents.

The following tables show the requirements, or lack of requirements, for certain classified matter protection and control procedures. Several points in time were selected to demonstrate the changes in requirements from 1988 to 1998. The 1988 requirements are used as a baseline because, in that year, DOE required accountability procedures and receipting and reproduction requirements that applied to all Secret and Top Secret documents. The requirements for Secret documents for 1992 are shown because in that year DOE modified accountability requirements for Secret documents. The 1992 requirements for protecting and controlling Secret documents have not changed.

Table 1 shows that many requirements for controlling Secret documents that were required in 1988 were discontinued in 1992. Among those discontinued were DOE's requirement to conduct inventories, maintain an accountability record, assign a unique identification number and copy and series to each Secret document, use receipts for the dissemination of Secret documents within a facility, and obtain approval from the document's originator before reproducing a Secret document. The requirements for retaining receipts and destruction documentation did not change. DOE has not and does not require a sign-out sheet for Secret documents.

Table 1: Changes in Minimum Requirements for Controlling Secret Documents

Control requirement	1988	1992
Frequency of inventories	Every 3 years	Requirement discontinued
Accountability record	Required	Requirement discontinued
Unique identification number	Required	Requirement discontinued
Copy and series designation	Required	Requirement discontinued
Receipts for internal distribution	Required	Requirement discontinued
Receipts for external distribution	Required	Required
Retention of receipts	2 years	2 years
Retention of destruction records	2 years	2 years
Approval for reproduction	Required	Requirement discontinued
Sign-out sheets	Not specified	Not specified

Source: Prepared by GAO on the basis of DOE documents.

Table 2 shows DOE's requirements for safeguarding Top Secret documents in 1995 and 1998 in addition to the 1988 baseline requirements. The requirements in 1995 are included because DOE revised its classified matter protection and control

manual, changing several inventory and accountability requirements. DOE decreased the frequency of inventories from semiannually to annually. DOE had also discontinued the requirements for assigning a copy and series designation to each document and the requirement for verifying that all Top Secret documents had been returned to storage at the end of the work day.

DOE's minimum requirements for 1998 are included because DOE again revised its classified matter protection and control manual to eliminate additional accountability requirements for Top Secret documents. In 1998, DOE eliminated requirements for performing annual inventories, maintaining an accountability record, assigning a unique identification number to each document, assigning a Control Officer, maintaining an access record, using receipts for the dissemination of Top Secret documents within a facility, and obtaining approval before reproducing a document. The requirements for using receipts for dissemination of Top Secret documents to recipients outside the facility and retaining receipts and destruction documentation did not change. DOE has not and does not require a sign-out sheet for Top Secret documents. The 1998 requirements for protecting and controlling Top Secret documents have not changed.

Table 2: Changes in Minimum Requirements for Controlling Top Secret Documents

Control requirements	1988	1995	1998
Frequency of inventories	Every 6 months	Annually	Requirement discontinued
Accountability record	Required	Required	Requirement discontinued
Unique identification number	Required	Required	Requirement discontinued
Copy and series designation	Required	Requirement discontinued	No change from 1995
Top Secret Control Officer	Required	Required	Requirement discontinued
End-of-day verification	Required	Requirement discontinued	No change from 1995
Access record	Required	Required	Requirement discontinued
Receipts for internal distribution.	Required	Required	Requirement discontinued
Receipts for external distribution.	Required	Required	Required
Retention of receipts	5 years	5 years	5 years
Retention of destruction records.	5 years	5 years	5 years
Approval for reproduction	Required	Required	Requirement discontinued
Sign-out sheets	Not specified	Not specified	Not specified

Source: Prepared by GAO on the basis of DOE documents.

While we were asked to discuss document protection and control within DOE protected areas, it should be noted that Secret and Top Secret documents stored outside of these areas require additional protective measures. In addition, these requirements have not been discontinued for some specific types of Secret and Top Secret classified documents. These include classified documents related to special access programs, cryptographic information, and NATO classified information.

I would like to reiterate that the requirements we address today are DOE's minimum requirements. The contractors who operate DOE's facilities may require additional controls and procedures to protect and control classified documents. In addition, as you know, we have recently begun our work for the Subcommittee related to accountability for classified documents and will be doing further work on these issues.

We discussed the information related to classified matter protection and control requirements with DOE's Office of Safeguards and Security and Office of Independent Oversight and Performance Assurance officials, who agreed with its factual accuracy.

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

Contact and Acknowledgements

For future contacts regarding this testimony, please contact Jim Wells at (202) 512-3841. Individuals making key contributions to this testimony include William F. Fenzel, Kenneth E. Lightner, Jr., and Ilene M. Pollack.

Mr. UPTON. Thank you.

Mr. Podonsky.

TESTIMONY OF GLENN S. PODONSKY

Mr. PODONSKY. Thank you, Mr. Chairman. I appreciate the opportunity to appear before this subcommittee to discuss classified information security controls at DOE's nuclear weapon laboratories. As you all are aware, my office provides the Secretary of Energy with an independent view of the effectiveness of departmental policies, programs and procedures in the areas of safeguards and security, emergency management and cyber security.

At the outset of my statement, I believe it is particularly important to inform this committee about some significant aspects of DOE's current administrative requirements for protecting classified information and how those requirements came about.

Ten years ago, DOE required a formal accountability system for all Secret and Top Secret information. Each document or item was accounted for from origination to destruction, and each was identified by unique number, page count, and various other specific markings. A chain of custody was maintained throughout the item's life. Additionally, periodic inventories were required to ensure that all documents or items were present and or accounted for.

In 1991, DOE began modifying its requirements for classified matter accountability. This action was in response to a governmentwide initiative that originated from a 1990 National Security Council assessment, intended to establish a single security program that could be applied to both industry and government.

Consequently, in February 1991, DOE modified its policy to eliminate the requirement to account for Secret-level national security information, which was not directly related to nuclear weapon information.

In May 1992, DOE again modified its requirements based on the provisions of part 2001 of Title 32 of the Code of Federal Regulation; this time eliminating formal accountability requirements for Secret RD; that is, nuclear weapons-related information.

In January 1998, under the authority of Executive Order 12958 dated April 1995, DOE eliminated security accountability requirements for all Top Secret information stored in secure areas.

With these modifications, current DOE policy only requires sites to formally account for certain types of documents, such as sensitive compartmented information, foreign government information, some sensitive nuclear weapons use control information, and special access program information.

These reductions of accountability requirements were part of a general trend toward reduction in security that occurred in the early to mid-1990's. During that period, DOE initiatives were aimed at reducing security costs, declassifying information and increasing openness at DOE sites. That general trend included DOE's encouragement for sites to reduce security costs through such actions as downsizing protective forces, downgrading clearances and eliminating or consolidating security areas, all elements of the overall program for protection of classified information.

However, as we have seen, security requirements subject to a wide range of interpretations do not enhance the security posture of our entire government. In response to the 1999 allegations of espionage at Los Alamos, Secretary Richardson took some extensive

and unprecedented actions. Security within DOE, and particularly at the three national weapons labs, received high-level management attention. Secretary Richardson directed the implementation of an extensive set of cyber security enhancements; strengthened DOE security management organization through functional reorganizations, in addition to personnel and expertise; elevated the oversight function to be a direct report to his office; implemented a polygraph program and issued a zero tolerance policy for security violations.

At the same time, the Headquarters Office of Defense Programs published a "goal post" document that established expectations for near-term improvements that would enable each site to achieve a satisfactory security program. Under these initiatives, DOE sites took aggressive action and strengthened their security programs and practices in several areas, including cyber security, control of foreign nationals and storage of classified weapon components. However, since these efforts were initiated within the DOE, they did not address the governmentwide policy problems associated with the control of Secret and Top Secret classified information.

DOE is unique in that it possesses and is responsible for safeguarding certain types of information that no other agency possesses; specifically, information categorized as restricted data that deals with nuclear weapons design, manufacture and testing, and includes information about disabling or enabling nuclear weapons. Such information merits a higher degree of protection than any types of classified information.

Consequently, at the direction of Secretary Richardson, DOE is currently evaluating and/or implementing four departmental-wide recommendations:

First, reinstitute requirements for a formal accountability system for Top Secret and Secret weapons data.

Second, establish a clear and comprehensive graded approach for information protection and issue appropriate implementing guidance. This approach should include practical guidelines for determining relative importance of information, provide more sensitive information and greater amount of protection.

Third, clarify the need-to-know policy in order to better limit access to information.

Fourth, continue efforts to expand the human reliability programs to include personnel with access to the most sensitive nuclear secrets.

When the Secretary was informed in June of this year of the security incident at Los Alamos involving missing classified hard drives, he demanded to get to the bottom of the situation and once again he took a number of aggressive steps to increase the control and protection of particularly sensitive weapons-related data.

The Secretary directed immediate implementation of several recommendations. Other recommended changes, including the four I specifically mentioned, should be incorporated—and these should be incorporated into DOE orders as soon as possible.

Additionally, he directed my office to make an immediate assessment on an expedited basis of the adequacy of security procedures and administrative controls for such information at Los Alamos, Livermore, and Sandia National Laboratories. We completed re-

views of Livermore and Sandia and we will conduct a similar review at Los Alamos after the FBI has completed its criminal investigation surrounding the classified hard drives.

This concludes my comments. Thank you, Mr. Chairman.

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

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

Thank you Mr. Chairman. I appreciate the opportunity to appear before this subcommittee to discuss classified information security controls at DOE's nuclear weapons laboratories. As you are aware, my office provides the Secretary of Energy with an independent view of the effectiveness of departmental policies, programs, and procedures in the areas of safeguards and security, emergency management, and cyber security.

At the outset of my statement, I believe it is particularly important to inform you about some significant aspects of DOE's current administrative requirements for protecting classified information and how those requirements came about.

Historical Summary

Ten years ago, DOE required a formal accountability system for all Secret and Top Secret information. Each document or item was accounted for from origination to destruction, and each was identified by a unique number, page count, and various other specific markings. A chain of custody was maintained throughout the item's life. Additionally, periodic inventories were required to ensure that all documents or items were present or accounted for.

In early 1991 DOE began modifying its requirements for classified matter accountability. This action was in response to a government-wide initiative that had as its foundation a 1990 National Security Council assessment intended to establish a single efficient national industrial security program that could be applied to both industry and government.

Consequently, in February 1991 DOE modified its policy to eliminate the requirement to account for Secret level information that was categorized as National Security Information—that is, information that could impact national security but was not directly related to nuclear weapons design or nuclear material production.

In May 1992, DOE again modified its requirements based on the provisions of Part 2001 of Title 32 of the Code of Federal Regulations, this time eliminating formal accountability requirements for Secret Restricted Data—that is, nuclear weapons-related information.

In January 1998, under the authority of Executive Order 12958 of April 1995, DOE eliminated accountability requirements for all Top Secret information.

With these modifications, current DOE policy only requires sites to individually account for certain types of documents, such as sensitive compartmented information, foreign government information, some sensitive (nuclear weapons) use control information, and some special access program information.

These reductions of accountability requirements were part of a general trend toward reduction in security that occurred in the early to mid 1990s, partly as the result of the end of the cold war. During that period DOE initiatives were aimed at reducing security costs, declassifying information, and increasing "openness" at DOE sites to promote interactions with local communities and with industry. That general trend included DOE's encouragement for sites to reduce security costs through such actions as downsizing protective forces, downgrading clearances, and eliminating or consolidating security areas, all elements of the overall program for protecting classified information.

In response to the 1999 allegations of espionage at Los Alamos, Secretary Richardson took some extensive and unprecedented actions. Security within DOE, and particularly at the three national weapons laboratories, received high-level management attention. Secretary Richardson directed the implementation of an extensive set of cyber security enhancements, strengthened DOE's security management organization through functional reorganization and addition of personnel and expertise, elevated the oversight function to a direct report to his office, implemented a polygraph program, and issued a zero tolerance policy for security violations. At the same time, the Headquarters Office of Defense Programs published a "goal post" document that established expectations for near-term improvements that would enable each site to achieve a satisfactory security program. Under these initiatives, DOE sites took aggressive action and strengthened their security programs and practices in several areas, including cyber security, control of foreign national visi-

tors, and storage of classified weapons components. However, since these efforts were initiated within DOE, they did not address the government-wide policy deficiencies associated with the control of Secret and Top Secret classified information. **Minimal security requirements that are subject to a wide range of interpretations for the purpose of implementation do not, as we have seen, enhance the security posture of our government.**

Recommendations

DOE is unique in that it possesses and is responsible for safeguarding certain types of information that no other agencies possess—specifically, information categorized as Restricted Data that deals with nuclear weapons design, manufacture, and testing, and includes information about disabling or enabling nuclear weapons. Such information merits a higher degree of protection than other types of classified information (categorized as National Security Information).

Consequently, at the direction of Secretary Richardson, DOE is currently evaluating and/or implementing four Department-wide recommendations:

- **First, re-institute requirements for a formal accountability system for certain types of information (i.e., Top Secret and Secret Weapons-Related Data).**
- **Second, establish a clear and comprehensive graded approach for information protection and issue appropriate implementing guidance.** This approach should include practical guidelines for determining relative importance of information; provide more sensitive information greater protection, and apply recent enhanced requirements for vaults to other storage containers.
- **Third, clarify the need-to-know policy.** In order to better limit access to information, DOE needs to determine prudent measures for identifying specific need-to-know for access to information and establish expectations for partitioning information stored in large repositories.
- **Fourth, continue efforts to expand the human reliability programs.** DOE's human reliability program, which includes drug testing and regular medical evaluations and ensuring that personnel who handle nuclear weapons and special nuclear material are reliable and fit for duty, should be expanded to include personnel with access to the most sensitive nuclear secrets.

When the Secretary was informed in June 2000 of the security incident at Los Alamos involving missing classified hard drives, he demanded to get to the bottom of the situation and, once again, he took a number of aggressive steps to increase the control and protection of particularly sensitive weapons-related data. The Secretary directed immediate implementation of several recommendations. Other recommended changes, including the four I specifically mentioned, should be incorporated into DOE orders as soon as possible to ensure that they are institutionalized and become part of a permanent policy base.

Additionally, he directed my office to make an immediate assessment, on an expedited basis, of the adequacy of security procedures and administrative controls for such information at Los Alamos, Lawrence Livermore, and Sandia National Laboratories. We completed reviews of Lawrence Livermore and Sandia, and we will conduct a similar review at Los Alamos after the FBI has completed its criminal investigation surrounding the classified hard drives.

That concludes my comments. Thank you, Mr. Chairman.

Mr. UPTON. Thank you both.

Mr. Wells, as I read your testimony back in Michigan, I came back last night after being back for the July 4 break, I was, I have to say, a little astounded at looking at the charts that you shared here and were part of your testimony, and I know that we are going to be asking Mr. Glauthier questions about some of this. But did you get any response back from DOE in terms of how they could change some of these requirements in the past years?

I mean, I look at myself back home and actually I do a fair amount of the grocery shopping. There is one store there called Myers, and they now have checkout lines where there is no cashier. You verify it yourself. It is scanned yourself. They have an absolute record in terms of the inventory of the store, and for those that hadn't done it before, I think there is one person for every four or five lanes going out.

When I look at no sign-out sheets, unique identification numbers requirement discontinued, I mean just a whole series of things, it is rather amazing when I see these changes that in my view have weakened our security, particularly with security lapses. I know a number of members went out to look at the labs. At least from my perspective, I was very impressed with the physical security, the swat teams that are out, ready to defend against the mission impossible days that we saw on TV a number of years ago. But it was the cyber security, the Wen Ho Lee case, other things, that trouble us the most. By discontinuing a number of things that were once in place, it seems that we have provided perhaps an open invitation to losing documents as we saw with the two hard drives.

What is your comment with regard to that? What reaction do you have?

Mr. WELLS. Regarding my reaction, when the committee inquired about GAO coming forth in a week or 2 to testify on what they had found so far, my audit team presented the results that you see on that chart, I did not believe them. I was somewhat concerned that I wanted the audit team to go back and verify and double-check. I found, like yourself, that I was astounded.

Given the problems that we are now seeing across the complex, it is unclear to us what objective was trying to be achieved when these requirements were reduced. We have not been able to document why some of these changes have occurred yet. Quite frankly, we asked for documentation for 1992, for instance, in the security Secret area, why all of those accountability-type requirements were dropped, and the Department supplied us with a single one-page memorandum that basically acknowledged that accountability requirements are being modified. Nowhere on this single sheet of paper is there any discussion of why these requirements were being dropped. So as of this moment, we still don't have a good handle on the why part.

Mr. UPTON. You know, one of the concerns that I saw with your testimony, and with particularly these two missing hard drives, I mean as we learned what was on those hard drives, I can't imagine a more important document that was missing. For the life of me, I don't understand why it was classified as Secret versus Top Secret. I will get to that a little bit later. And Top Secret obviously ought to have a higher classification in terms of its tracking and its whereabouts.

Do you have any idea why the Top Secret control officer, which you mentioned in your testimony, was dropped?

Mr. WELLS. No, sir, I don't have a good answer for you yet.

Mr. UPTON. Mr. Podonsky, do you have a reaction to those first two questions, these charts and the Top Security control officer?

Mr. PODONSKY. Well, we can confirm that what the GAO is reporting is an accurate portrayal in terms of the requirements. But I think part of what we have found over the years, and we have a long history in 1991, 1992, 1993, 1994, regarding concerns about the policy, is that this was a clear national initiative back in 1990; and there is a long stream of documentation that outlines how this came about, starting with President Bush's request of the National Security Council to prepare a review of how to consolidate into a

single security program an industrial requirement that the government could align itself to.

It finally resulted in a National Industrial Security Program Manual that came out in 1995 that lays out this. Why the Department elected over the years to continue to change its requirements, that's not clear. I would have to yield to the policy arm of the Department.

Mr. UPTON. I know we are going to have a couple of rounds so I am going to try to stick to the 5 minutes.

Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. Wells, I am looking at page 3 of your testimony. You are talking about DOE's requirements over the past 12 years. It starts off, and in the first paragraph, middle of the paragraph, it reads, According to DOE classified matter protection and control officials, these changes were implemented to promote governmentwide uniformity among contractors and to account for technological changes such as computers, copiers, and faxes in the processing and storage of classified information. In our ongoing evaluation, we will be looking at how other agencies protect and control classified documents."

So these changes that have occurred over the last 12 years was to make everybody—contractors, the government, DOE, the labs—all get on the same page? Am I reading that right?

Mr. WELLS. That's correct. We are talking about CIA, Department of Defense.

Mr. STUPAK. National security?

Mr. WELLS. National security agencies.

Mr. STUPAK. So that started back in about 1988?

Mr. WELLS. It was begun then; yes, sir.

Mr. STUPAK. When you go to make everybody on the same page, isn't that when, really, breaches of security start to break down; or start to occur, I should say?

Mr. WELLS. Clearly, from what we understand, much of the discussion that occurred in terms of whether that would work or not was centered on unique requirements that may exist in individual agencies under different circumstances. There were many people that did not agree with that initiative for uniformity. That's what we understand.

Mr. STUPAK. Well, do you agree with this need for uniformity amongst contractors and government and private industry and DOE and NSA? Should they all be on the same page, or should there be different degrees of security as you move forward within government or within industry, depending on the weapon or the research you are doing?

Mr. WELLS. I agree that GAO as an audit team will go in and continue to look at the reasons why the requirements may or may not need to be different throughout the agencies, but clearly we shouldn't lose sight of the objective of all security protection is to prevent the loss and prevent the compromising of material. And what we are currently seeing, the existing uniformity of regulations are not achieving that objective. So we may have a situation where we need to look at some unique requirements, particularly as regards to our nuclear weapons.

Mr. STUPAK. Okay. But in answer to my question, do you agree that they all should be on the same page or should it be different?

Mr. WELLS. I am unable to agree or disagree until we have had a further chance to further investigate.

Mr. STUPAK. I thought GAO's job was to evaluate this situation and to give us some recommendation to give this committee and others, oversight, as to how we should approach these things?

Mr. WELLS. Absolutely. We have an ongoing audit and investigation. We have been in it about 3 weeks. That work is continuing and we hope to have that work finished for the full committee and this subcommittee shortly.

Mr. STUPAK. But over the last 3 weeks, obviously you have done more—other audits; because going back to 1976, I think Mr. Dingell started the first letters, and periodically every 2 years he was on GAO to do an investigation, to do an audit because things weren't working right with the secrecy of our top secrets in this country.

Mr. WELLS. Clearly, GAO has a history of 20 years of oversight in classified security matters and each and every time we have gone in and looked, there have been problems. Each and every time we have heard corrective action being promised by the Department of Energy. When we have looked at some of these, we have found that the implementation has not been as successful and problems seem to be recurring.

Mr. STUPAK. When you would look at it and you would see problems recurring over the last 20 years, you would make your recommendations and go back and see it was never done?

Mr. WELLS. We have made 50 recommendations in the last 20 years. I had my team count up the number of recommendations that have been reported.

Mr. STUPAK. You have had 50. How many of them were carried out?

Mr. FENZEL. I can answer that. In almost all cases with our recommendation, what DOE does is agree with the recommendations, take corrective action; but then what happens is things start to change and the implementation of the recommendation falls through and the problem resurfaces.

Case in point with the classified documents: We issued a report in 1991 that pointed out missing classified documents. At Lawrence Livermore over 10,000 documents were missing. At other facilities at DOE, hundreds of documents were missing. DOE agreed, said they had a problem with controlling classified documents and were going to institute tighter controls.

A year after that is when they began reducing the requirements for Secret. So the history is they take corrective action, but then in the implementation that corrective action usually falls down in many cases.

Mr. STUPAK. So we hear your recommendations; we agree with those recommendations; we begin to implement it, but the wheels come off the cart halfway through?

Mr. FENZEL. A year, 2 years down the road, a lot of security issues are cyclical in this fashion.

Mr. STUPAK. How long—if anyone knows, how long has the longest Secretary of Energy ever been in the position? It seems to be like a resolving door there with Secretaries of Energy.

Mr. FENZEL. A lot of them. The tenure of the Secretary of Energy—we did some work on that about 2 years ago. I can't comment on the present Secretary's tenure, but on average it is usually less than 2 years.

Mr. STUPAK. Less than 2 years?

Mr. FENZEL. Right.

Mr. STUPAK. So there really is no accountability or responsibility going on when we have a revolving door at the top, is there?

Mr. FENZEL. I think that hinders any type of security.

Mr. STUPAK. Thanks.

Mr. UPTON. Mr. Burr.

Mr. BURR. Mr. Fenzel, after doing your assessment for the GAO, can you sum up in a couple of sentences not what you found, but what you felt like after you finished?

Mr. FENZEL. You mean this present assessment?

Mr. BURR. Yes, sir.

Mr. FENZEL. Our work is still ongoing. And I can verify that when our boss, Mr. Wells, did get these tables, he didn't believe us at first. So in a way, we had to convince him that this was the situation.

As for my reaction, I was more concerned on the Top Secret situation and the decreases in requirements there.

I would like to put a caveat on that. These are the minimum requirements of DOE. The laboratories can do a lot more, and I think what you will probably hear is that there are other things they are doing beyond the minimum controls.

My problem is that these are the minimum controls and while there are more controls out there right now, they are not necessarily going to be followed 1 year from now, 2 years from now, 5 years from now, and that eventually if these minimum controls are kept in place, somebody, somewhere, is going to follow these minimum controls and that's——

Mr. BURR. Let me read you something from Mr. Podonsky's review. It is found on page 17. It says—it is talking about various DOE elements and individuals that advocated reestablishment of formal accountability systems for Top Secret documents and Secret weapons data.

Most noticeably, March 1999, the director of the three nuclear weapons laboratories sent a joint recommendation to the DOE Under Secretary and the DOE Director of the Office of Counterintelligence in which they advocated that DOE reinstate accountability for documents that contained Secret restricted data and Top Secret restricted data.

Would it surprise you that the lab directors were on record in March 1999 saying we want to reinstitute this?

Mr. FENZEL. Well, that doesn't surprise me.

Mr. BURR. It doesn't surprise you, does it?

Mr. FENZEL. No.

Mr. BURR. Let me ask you, Mr. Podonsky—let me just read the conclusion of that paragraph:

They indicated that without formal accountability, counterintelligence reviews are much more difficult because it is not feasible to determine specifically who had had access to certain design information. They also cite the Cox Commission report as a basis for reinstating formal accountability.

I mean, is that an accurate depiction in your report of the lab directors and their requests?

Mr. PODONSKY. As far as we know, everything that we put in our report is valid.

Mr. BURR. Is it not difficult to turn around and blame the lab managers if they have been out there formally requesting reinstituting some of the accountability methods? I am not saying that you are accusing them, but there certainly are some.

Mr. PODONSKY. Congressman Burr, as you have heard me state, we have been in this Department—I have been in the Department for 16 years, and we have been writing on a lot of these issues for as many years as I have been here. So clearly there is a frustration that there is a tendency in the Federal Government that there is always fingerpointing as to who is responsible. And clearly in our collective opinion, from an oversight, laboratories have the responsibility and so does DOE. There is a shared responsibility here. As our colleagues from GAO have pointed out, is the requirements don't say that you can't go above what those—what the standard is. You can raise the bar. In some cases the labs have done that.

Mr. BURR. They in fact have, and I think you point out very clearly in your report, and let me just read on page 6: The current national requirements for controlling classified matter are not as stringent and clear as needed in light of DOE's particularly sensitive nuclear weapons-related information. Improvements in policy are needed to further enhance security at DOE sites.

And then on page 10: In many cases in the past, independent oversight had determined that sites were complying with the established requirements but that the security interests were not provided sufficient protection because the applicable DOE policies are not sufficiently clear or comprehensive.

I guess I would ask of you, given that they had exceeded where they thought they understood it in the other areas, how much of a problem was the fact that the guidelines were unclear or that improvements in the policy were needed?

Mr. PODONSKY. We believe that clearly there can be more granularity to the DOE requirements so people understand, without exception, what the requirements are meant to be. However, we also believe that there is—while you can have good policies, it is also the implementation of those policies. So there are two sides to this: How are the policies being implemented? And are the policies really clear?

Mr. BURR. I am going to respect the chairman's time.

Mr. UPTON. You better.

Mr. BURR. It is not too difficult to understand if a lab director says we didn't know something was our responsibility. There are some things that are unclear relative to the guidelines where one might understand how they came to that conclusion; is that accurate?

Mr. PODONSKY. I think in some areas you can say that, but mostly I would harken back to there needs to be a core value of security applied, just like safety. It is everybody's responsibility, and the fact that people have a clearance, they have accepted a certain responsibility, and that means accountability as well.

Mr. BURR. I think the lab directors will agree with you, as would these members.

I yield back, Mr. Chairman.

Mr. UPTON. Dr. Ganske.

Mr. GANSKE. I would like to go to this chart for a few minutes. Some things I think are self-explanatory. Frequency of inventories in 1988, every 6 months; in 1995, annually; and then 1998, requirement discontinued. Accountability record required in 1988 and 1995, and then discontinued.

Unique identification number, I think probably everyone understands. What does the Top Secret control officer do or did?

Mr. WELLS. A Top Secret control officer was basically performing custodial duties and was ultimately charged with the responsibility for Top Secret documents. He was the accountable guy. He was the one that said, I know where this document is; I know where it is stored; I know who had it, and I know when it was put back. That was the basic thrust of that position responsibility.

Mr. GANSKE. And that——

Mr. WELLS. Top Secret.

Mr. GANSKE. [continuing] control officer was able to do that because he or she had end-of-the-day verification?

Mr. WELLS. He had a responsibility to certify at the end of each day.

Mr. GANSKE. Had an access record?

Mr. WELLS. Who was entitled to look at a document or check a document out.

Mr. GANSKE. And there were receipts for internal distribution?

Mr. WELLS. That's correct.

Mr. GANSKE. But those things were discontinued in 1998?

Mr. WELLS. 1992——

Mr. GANSKE. Some were discontinued in 1995?

Mr. WELLS. Yes, Top Secret, some in 1995.

Mr. GANSKE. And some in 1998?

Mr. WELLS. Yes, some in 1998.

Mr. GANSKE. Then we have here, approval for reproduction, copying documents, in 1988, required; 1995, required; in 1998, requirement discontinued.

Mr. WELLS. Discontinued, that's correct.

Mr. GANSKE. Where was this copy machine that the disk drives were found behind? Where was that located?

Mr. WELLS. We don't know that. We are basically waiting for the investigative team to get through. We understand it might—well, do you know?

Mr. PODONSKY. No, we have not been into the area of X division since the investigation started.

Mr. GANSKE. Doesn't it strike you gentlemen as sort of unusual that we have a copy machine there, we don't have any method to determine who is checking out this stuff or copying it, taking copies wherever? Not very good security, is it?

Mr. WELLS. It does not appear to be. Even if you were an originator of the document, the intent was to ensure that your document—you became aware of how many of those documents were out there and who had them. Even that's been lost.

Mr. GANSKE. All right. Well, we had a bunch of changes here in 1995, and then in 1998. The Secretary of Energy back in 1995 was Hazel O'Leary. Did she give—did she sign off on these changes? Do you know whether she did or did not?

Mr. WELLS. The 1995 date was to correspond with the revision of DOE's security manual. So whichever office secretary signed the security manual in 1995, which again was updated and there were additional changes in 1998, it was put out under a DOE cover and was signed by some top official in the Department of Energy. I don't have those documents with me.

Mr. GANSKE. So I mean, it could have been an Under Secretary?

Mr. WELLS. Yes, that's correct.

Mr. FENZEL. It could have.

Mr. GANSKE. Should not something of this importance also be reviewed by the Secretary? Would any of you care to answer that?

Mr. PODONSKY. From my experience in the Department, up until this Secretary, and with the exception of Admiral Watkins in the 1990 period, we did not have a Secretary that really focused on security in the Department.

Mr. GANSKE. Okay. Well, 1998, I believe the Secretary was Mr. Pena. Is that correct?

Mr. WELLS. Yes.

Mr. GANSKE. Okay. So we had a whole bunch of requirements discontinued in 1998. Am I to assume that Mr. Pena did not sign off on these, or do you know?

Mr. PODONSKY. I don't know.

Mr. WELLS. I do not know.

Mr. GANSKE. Would it be your recommendation that when we are dealing with changes in security requirements that the Secretary take a personal interest and review these before this becomes Department policy?

Mr. WELLS. Absolutely. I think if anything, from a lessons learned standpoint of the many years we have looked at these problems, it continues to concern us—and I used the word "mindset" that was mentioned earlier—about the lack of attention and perhaps lack of a priority that's been placed on some of these security matters.

Mr. GANSKE. One last question, Mr. Chairman.

Now, you mentioned an Executive Order, I believe, in your testimony, that was for changes. When was that Executive Order issued? Was it 1995, 1998?

Mr. PODONSKY. There is an April 1995 Executive Order entitled Classified National Security Information, and that was April 17, 1995, that was issued.

Mr. GANSKE. Okay. Now that's signed by the President, right?

Mr. PODONSKY. Correct.

Mr. GANSKE. The President should receive, you know, a recommendation, I would think, from the Secretary of the Department of Energy before he would sign an Executive Order like this. Would that be your impression?

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

Mr. GANSKE. Do we know whether that happened or not?

Mr. PODONSKY. We have not seen any paper trail to that effect.

Mr. GANSKE. Are you looking for that, for this committee to try to find out how to improve this situation in the future?

Mr. PODONSKY. We issued an interim report, as you probably are aware, and when we continue on with the Los Alamos piece we will complete the whole package and one of the things that we have is we are trying to put together the entire trail from 1990, from the original President Bush direction on the National Security Council to present, as to how this whole thing evolved.

Mr. GANSKE. Is it your current recommendation that these discontinued requirements be reinstituted?

Mr. PODONSKY. That's our recommendation to the Secretary.

Mr. GANSKE. Has that—what has happened since your recommendation?

Mr. PODONSKY. The Secretary's response to our report was to immediately turn to the policy folks and tell them that they need to take a look at implementing this right away.

Mr. GANSKE. Just to take a look, not to do it?

Mr. PODONSKY. They need to take a look at what the implications are going to be, so consequently they are—and I think the second panel can probably testify to more current what they are doing with those recommendations.

Mr. GANSKE. Since we have lost the disk drives there has not been a reinstitution of these requirements to date?

Mr. PODONSKY. No, there was guidance put out and requirements put out by the Secretary on June 19 and further followed up by General Habiger on June 23. So they did start tightening up right now.

Mr. GANSKE. Thank you, Mr. Chairman.

Mr. UPTON. Mr. Bryant.

Mr. BRYANT. Thank you, Mr. Chairman. You may have already stated this but I would ask unanimous consent to put my statement in the record.

Mr. UPTON. It has been done.

Mr. BRYANT. Thank you.

I thank the panel for being here and the second panel. I apologize for not being here on time and probably leaving early also because we do have conflicting committees, and we have to go back and forth between these.

Mr. Podonsky, you may have—I know we have been talking about this already around this subject, but you note in your report the absence of specific requirements, the Department of Energy sites often decide to implement only the minimum requirements because of cost concerns. Can you elaborate on this point and indicate whether you are aware of instances in which DOE or the sites have refused to fund proposed control requirements beyond this minimum standard?

Mr. PODONSKY. I realize in our report we talk about minimum standards, and perhaps it is the complexity of the English language but what we have found is that the—while the standards that are out there are needing of clarity that if implemented properly we think that they are good standards, they need to be raised to be—

account for what they call the graded approach so that different types of information can be afforded the protection commensurate with that sensitivity of the information that we are talking about.

But we have seen over the years that if left to open interpretation of what the requirements are, then we are basically, as an agency, leaving potential vulnerabilities as to whether enough is enough or when you have too much security applied.

So our recommendation to the Secretary and to General Habiger is that we recommend that they revisit and reinstitute an accountability system similar to what we had back in the early—the early 1990's and late 1980's. That's not to say that we don't want the Department to take into accountability the technology that can be used today, but clearly accountability of some of our most sensitive information needs to be reinstated.

Mr. BRYANT. I think I agree with you. I notice that you mentioned specifically problems with lack of specificity and clarity in DOE orders, and then combined with the system I would say minimum requirements and couple that with the cost reimbursement nature of DOE's contracts with labs, this all seems to work together in effect to create a race to the bottom, so to speak, on the security issues.

Again, Mr. Podonsky, could you address this need-to-know issue and what more needs to be done by the Department of Energy and the labs in this area?

Mr. PODONSKY. Need to know is an old standing requirement of a lot of government agencies dealing with sensitive information, and our position with the Department is that the need to know needs to have some additional clarity to it for individuals that have the responsibility. Say for a program manager in a vault, if that custodian or program manager needs to be able to determine who has access to that vault, need to know needs to be established, but rather than just limit it to the individual accountability and saying, okay, you are the manager, you determine what need to know is, we think there needs to be a little higher degree of granularity as to what the Department expects.

For example, and this is just an example, if somebody has daily access to information, they probably have a need to know, but if they only have occasional need for that information perhaps they don't have a regular need to know.

So that needs to be discussed further with the policy group in the Department of Energy, but we feel that need to know over the past couple of years has been left to pretty much the interpretation of the individuals that are executing that. And while they have the ultimate responsibility to execute that, we also think there needs to be clear guidance from the Department.

Mr. BRYANT. Do you—and my last question to you, are you satisfied with the Department's response to your recent recommendations on tightening controls on classified matter?

Mr. PODONSKY. We believe that the initial steps that the Secretary and General Habiger are taking are, in fact, in the right direction and we are going to be closely monitoring that. We would like to see a continued evolution of that.

Mr. BRYANT. Thank you.

Mr. UPTON. Thank you.

Mrs. Wilson, though not a member of the subcommittee but a member of the full committee, you have been allowed to participate in other subcommittee hearings, I need to ask unanimous consent. Do you desire that?

Mrs. WILSON. Yes, Mr. Chairman.

Mr. UPTON. I would make a request, a unanimous consent request, that you may ask questions as part of this hearing today. Any objection?

Mr. STUPAK. No objection.

Mr. UPTON. Thank you. Mrs. Wilson, you are recognized for 5 minutes.

Mrs. WILSON. Thank you, Mr. Chairman.

I am interested in this question of policy and compliance with policy, and I note from the records from up here that General Habiger testified last month before the House Armed Services Committee that the national labs were in full compliance with DOE security policies. I believe that was before the most recent incident at Los Alamos.

And then we have a significant change in security policies on June 19. And subsequently some very specific changes to what the minimum requirements are on everything from data bases to vault security to whether things are classified properly and how to—how to encrypt data and so on and so forth.

Mr. Podonsky, is it your view as well that Los Alamos and Sandia and Lawrence Livermore were in compliance with the security policies at the time General Habiger testified to that?

Mr. PODONSKY. As exemplified by our most recent review that the Secretary directed at Livermore and Sandia and Los Alamos, the answer is, yes, we found that they were in compliance with the DOE, what we call the minimum requirements that the DOE has. Los Alamos we still need to go back up to, but we haven't finished that because of the FBI investigation. However, before you came in I also made a statement that you can be in compliance but it is also more—equally as important is how those requirements are being implemented. It's the practice that's also important. We can tighten up all of these requirements, and I hope that we do. I believe we will. But that still doesn't take into accountability the individual error that either is deliberate or by sloppy practice.

It is the human factor. These people that are cleared to have access to this information, have a need to work with information, and as long as they have that need to work with that information there is always going to be the reliance on the individual. That is something that you can never have an absolute.

Your question is, are they in compliance? Yes, as far as we can tell, they are in compliance.

Mrs. WILSON. But it was the Department of Energy's view that the standards needed revision following that incident. I guess what I am getting at is, they were in compliance with the standards before this happened. There has been a significant revision of standards by the Department of Energy after it happened. So really this is a question of what our security policy is in the Department of Energy, isn't it?

Mr. PODONSKY. And I would defer that to the second panel for General Habiger, but over the years, as I also made a statement

earlier, we have been encouraging the Department to, instead of going down the path from 1990 to where we are today of decreasing requirements but go back to the path that Secretary Richardson and General Habiger are now taking the Department in increasing the requirements.

Mrs. WILSON. Since when?

Mr. PODONSKY. Since 1991.

Mrs. WILSON. But we have seen the decline through 1998. I mean, since when have you been encouraging things to go back in the other direction?

Mr. PODONSKY. We have correspondence to the policy group of this Department from 1991, 1992, 1993, 1994, and again up until this past year a lot of what we were reporting on was not necessarily heeded.

Mrs. WILSON. In other words, you were ignored when you said we needed to have higher standards?

Mr. PODONSKY. I did not want to say that, but yes.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. UPTON. Thank you. We will start a second round.

Mr. Podonsky, I know that you have not been allowed to go back to Los Alamos while the FBI is conducting the investigation. Have you visited the other two labs?

Mr. PODONSKY. Yes, we have.

Mr. UPTON. What is your reaction as to trying to make sure that something like what happened at Los Alamos doesn't happen at one of the other two labs? Have they tightened up their security? Have they made some changes that would prevent something like the missing disks, the hard drives from happening again?

Mr. PODONSKY. Yes, sir. We believe that the other two laboratories that we reviewed in a very short period of time have tightened up their security, and we don't believe—especially with the further initiative that the Secretary directed on June 1, we don't believe that that is likely to happen. But, again, nothing is an absolute.

Mr. UPTON. Now, one of the chart lines, and I touched on this a little bit earlier, the Top Secret control officer is not a requirement. Do any of the three labs actually have a Top Secret control officer?

Mr. PODONSKY. At Sandia they are controlling TS and they have been controlling TS, Top Secret, and to a lesser extent at Livermore. Whether or not they have a Top Secret control officer, I don't know. I would have to find out.

Mr. UPTON. Okay. I want to read just a couple of comments from the redacted version of the GAO report and get your—from the Podonsky report, and get the reaction by both of you.

DOE policies make no real distinction between documents and electronic media with respect to storage and control. Most of the requirements in DOE orders were written before the advances in cyber technology and were primarily developed with paper documents in mind. There has been little revision of the orders or manual that reflect technology advances, and it goes on and says in some instances large vaults containing many types of information that had no additional partitioning such that anyone with access to the vault would have access to any of the information therein

with no explicit provisions for need to know, and a couple of pages later it says although there are some differences the minimum protection requirements for Top Secret are not significantly more stringent than those for Secret or Confidential.

Isn't that the bottom line problem that we had at Los Alamos? Mr. Podonsky?

Mr. PODONSKY. Yes, sir, it is.

Mr. UPTON. Do you believe that there—and Mr. Wells, do you have a comment in that regard, too?

Mr. WELLS. Clearly, you cannot think of fax machines, you cannot think of e-mails and then turn around and look at DOE's security manual, which clearly strikes you as being old fashioned and out of date.

Mr. UPTON. Have any of you seen any evidence that DOE's orders even acknowledge the dramatic changes that were under way with this information change in technology during that last number of years?

Mr. WELLS. No, we have not.

Mr. UPTON. Mr. Podonsky?

Mr. PODONSKY. We have seen anecdotal evidence that there are changes taken about as we inspect the cyber security.

Mr. UPTON. What did your teams observe with respect to how the other two labs were handling NEST material and other similar assets and what do you attribute those differences to?

Mr. PODONSKY. We did not go into great detail into the investigation into NEST because of the FBI desire to expand the scope of their investigation to include all NEST activities, but what we did look at, we did find that there was good procedures—that they were following the DOE procedures that were established.

Mr. UPTON. At some point—I mean, I don't know at what point the FBI will allow you back in, but are you planning to——

Mr. PODONSKY. Yes, sir, we are not only planning to go back to Los Alamos, we are also going to do a specific inspection of the entire NEST operation of all the locations that the DOE has.

Mr. UPTON. Do you expect that to happen in the next couple of weeks before the summer is out? What is your timetable?

Mr. PODONSKY. We expect to go back to Los Alamos at the time that we can go back in when the investigation is complete. In terms of the NEST inspection, we plan to do that before the fall.

Mr. UPTON. Had the hard drives been designated as Top Secret versus Secret, do you think they would have been missing?

Mr. PODONSKY. I don't have the information on what the particulars are in the investigation and whether they would have been missing or not.

Mr. UPTON. Mr. Wells?

Mr. WELLS. While I could not speculate, clearly looking at the two charts many of those document control requirements, whether it be Secret or Top Secret, are not a requirement. So one could speculate that they perhaps might still be missing.

Mr. UPTON. Thank you.

Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman. When I asked questions earlier, we sort of established that these minimum controls were not only in DOE but NSA, CIA, private contractors, correct?

Mr. WELLS. We were told that the changes that were initiated in 1992, 1995 and 1998 were in response to trying to get uniformity across the government, yes.

Mr. STUPAK. Sure. So the breaches we have had here in security in Top Secret could have happened in any one of these agencies, departments, even from private government—I mean private contractors, correct?

Mr. WELLS. We understand that the chart was prepared for only looking at and assessing the DOE orders. We, the GAO audit team, had not looked at the other DOD-type orders or requirements to confirm that they are similar.

Mr. STUPAK. Okay.

Mr. Podonsky, it could have happened somewhere else other than DOE?

Mr. PODONSKY. We believe that to be the case, irrespective of what the chart shows.

Mr. STUPAK. In fact, the Walker spy case did not involve DOE but that was one where they made copies of classified documents on copy machines and gave them away because we had these so-called minimum standards, correct?

Mr. PODONSKY. I believe that to be the case.

Mr. STUPAK. You are nodding your head yes, but you have to give something verbal so we can record it.

Mr. PODONSKY. Sure.

Mr. STUPAK. I know when I shake my head, it rattles once in awhile.

Mr. PODONSKY. Mine doesn't rattle, sir.

Mr. STUPAK. But the minimum controls, that would also apply to University of California and the labs, correct?

Mr. PODONSKY. Correct.

Mr. STUPAK. Even though the director of DOE may be—a Secretary may only be there less than 2 years, these contracts are 5 years so even if there is a change in Secretary, the contract still must be fulfilled by the labs to these minimum standards, correct?

Mr. PODONSKY. Correct.

Mr. STUPAK. Regardless of what the minimum controls are, I would hope that the labs don't feel that even though we have these minimum controls that does not give them a right to lose documents or to lose hard drives, things like that; correct?

Mr. PODONSKY. Correct.

Mr. STUPAK. And I would hope that if you are doing a contract, whether it is with the government or private industry, you would always try to perform to the maximum potential of a contract and not the minimum levels of a contract; correct?

Mr. PODONSKY. Correct.

Mr. STUPAK. All right. Mr. Podonsky, in your testimony you indicated that Secretary Richardson has put in four things, and I summarized them briefly as accountability, graded approach, need to know limited access and human liability. That is just when I was taking my notes there.

You have indicated that the graded approach to protecting classified material should be implemented. Under this approach, some Top Secret documents would have more restrictions than others. In the next panel, Mr. Aftergood is probably going to testify about the

higher fences initiative. Are you familiar with this, the higher fences initiative?

Mr. PODONSKY. I am vaguely familiar with the initiative.

Mr. STUPAK. Is this a similar concept to the graded approach?

Mr. PODONSKY. I believe it is.

Mr. STUPAK. Could you explain a little bit more clearly to me what you mean by this graded approach?

Mr. PODONSKY. The Department has in place and has had for some time now the concept of graded approach, which means that the sites have to protect documents according to the type of information that's there.

So, in other words, not all secrets that we hold in this country should be afforded the same type of protection. So the graded approach is meant to allow folks—allow the people that have to be accountable for the maintaining of these sensitive or classified documents at a higher level.

Mr. STUPAK. So the graded approach is not just the site specific but also what happens internally within that site?

Mr. PODONSKY. Yes.

Mr. STUPAK. Okay. Thank you.

Higher fences, if I remember correctly, was one of the recommendations of Secretary O'Leary's Interagency Fundamental Classification Review submitted in 1996. Since the Department of Defense shares much of this information, DOE has been negotiating, and I understand unsuccessfully, with the Department of Defense since 1997 over what should be included. But the whole effort appears to be dead at this point because DOD says it costs too much and has operational impact.

Can DOE implement the graded approach when DOD refuses to have the same level of security for the same documents if we are talking about these minimum requirements and graded approach? Can you apply it?

Mr. PODONSKY. General Habiger would be more equipped to answer that but I will answer that from our perspective, and irrespective of what DOD is willing to do or not do, I think this agency should take the initiative and raise the bar on its own requirements.

Mr. STUPAK. Okay. Thank you, Mr. Chairman. I will yield back.

Mr. UPTON. Thank you.

Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman. Mr. Chairman, I referred to a letter earlier from the lab directors to Secretary Moniz at the Department of Energy on 3-1-99. I would ask unanimous consent that that be entered into the record.

Mr. UPTON. Without objection.

[The information referred to follows:]

[faxed to Moniz 3/1/99]

Proposal to Reinstate the Formal Accountability for Documents that Contain Secret Restricted and Top Secret Restricted Data

Historically, US nuclear weapons program documents that contained nuclear weapons data were placed in access control categories and marked as Restricted data/Formerly Restricted data. Unlike corresponding documents at the Secret level within the Department of Defense, such documents within the Department of Energy were handled as accountable, and their custody was tracked throughout their lifetime. [Note: this level of accountability and tracking is equivalent to the controls in place for Top Secret documents within the DoD.] However, in February of 1995 the DOE eliminated these stringent controls on SRD documents. In January of 1998, accountability for Top Secret Restricted data documents was eliminated.

As we in the laboratories have considered the Cox Commission findings, it appears desirable to reinstate such controls, certainly for all Secret Restricted data and Top Secret Restricted data documents that contain weapons design data. We have noted that, without information on who has had access to certain design information, our counterintelligence reviews are much more difficult. Strict reinforcement of "need-to-know" requirements on access to weapons design information, with periodic reviews of exactly which personnel have had access to this information, should strengthen our counterintelligence efforts.

The directors of all three of the DOE nuclear weapons design laboratories are in agreement that the former controls should be reinstated as quickly as possible. This recommendation is presented to the Undersecretary and counterintelligence official, for their evaluation of what, if any, problems might result from prompt reinstatement of the previous policy.

Mr. BURR. Mr. Podonsky, you referred earlier to the fact that Secretary Richardson had implemented a number of new security policies, some recent, some last year, when the first incident at Los Alamos took place. One of them was the polygraph. Has anybody been polygraphed?

Mr. PODONSKY. Yes, sir. I can tell you personally that almost my entire office has been polygraphed.

Mr. BURR. Your office, the investigators have been polygraphed. From the standpoint of the original scope of who was to be polygraphed, individuals at the labs, has that taken place?

Mr. PODONSKY. I believe it has, and again I would defer to the second panel for the specific numbers.

Mr. BURR. I will be sure to cover it with them.

Let me go back to your report and again read from page 6. "Secretary Richardson has again taken prompt and aggressive action to address residual weaknesses that have become apparent in the course of security incidents. On June 19, 2000, the Secretary issued directions to enhance classified matter protection. For example, he specifically required nuclear weapons laboratories to immediately implement measures for better control entry and egress to vaults, including mandating that logs be kept."

I take it that was a directive from the Secretary that you are referring to?

Mr. PODONSKY. Yes, sir.

Mr. BURR. Let me ask you, if the labs were responsible for security, why would it need a secretarial mandate or referral to address specifically those vaults?

Mr. PODONSKY. Well, because since there was no requirement prior to that.

Mr. BURR. But there was a request prior to that, correct?

Mr. PODONSKY. I am not following the request.

Mr. BURR. Did you find at any time that any of the labs had tried to upgrade the security to their vaults?

Mr. PODONSKY. There were anecdotal examples that the teams have found that they were upgrading at Sandia and to a lesser extent to Livermore.

Mr. BURR. In one case, if I remember, at Sandia, it was met by the Albuquerque office with "we won't pay for the upgrade in security."

Mr. PODONSKY. I am not familiar with that.

Mr. BURR. We will get into that later. Let me again go to your report on page 14. "The recent independent oversight review concluded that the laboratories had addressed identified weaknesses," parenthesis, "including long-standing weaknesses with classified parts, met DOE's expectations defined in the goals posted in the goal post memorandum and generally met current DOE requirements."

Now we are talking about moving the security totally outside of these contractors and possibly renegotiating a contract with contractors where security is done by a third party, I take for granted, is the initiative. Let me just ask you, honestly, will this work if that's all we do?

Mr. PODONSKY. I guess, Congressman, to get to the heart of the answer to your question, I would say that no matter what we put in place, in this Department or any other agency, it goes back down to whether people are going to be held accountable for violating practices, how those practices are put into place. If you go to a third level contractor, I can only give you a personal opinion, and my personal opinion is it is dependent on the management of that contract and how people are held accountable for that contract.

We have seen a variety of examples of contracts in the Department. Some work better than others. A lot of it is driven by the individual at the top.

Mr. BURR. Have you ever done an evaluation or study of the Albuquerque office as related to their involvement in the security at the two labs they are responsible for?

Mr. PODONSKY. Yes, sir, we have.

Mr. BURR. And what was your finding, if you could just summarize that?

Mr. PODONSKY. Dependent on who the field office manager was at the time which is responsible for the Albuquerque operation, we found varying degrees of effectiveness from the Albuquerque office.

Mr. BURR. Is it safe to say that Albuquerque was fully aware of the intricacies of the NEST program?

Mr. PODONSKY. I don't know.

Mr. BURR. Would they have been fully aware of the security requirements that the labs instituted at the vaults?

Mr. PODONSKY. They should be, because they are required to do an annual survey of the lab.

Mr. BURR. Is it safe to believe that Albuquerque DOE office knew that that particular vault had shared resources in it?

Mr. PODONSKY. I would assume that since the Albuquerque office, as I said, does the annual survey of its sites that they should have known what was contained in that vault.

Mr. BURR. Have you ever found anything that would suggest that the Albuquerque office had concerns about the security procedures in place at Los Alamos, specifically that vault?

Mr. PODONSKY. Not specifically that vault.

Mr. BURR. NEST program?

Mr. PODONSKY. I have not been made aware of that.

Mr. BURR. Is it safe to assume that Albuquerque knew that at least in Los Alamos, and I believe true in all of the—in Sandia as well, and I am sure I will be corrected later, knew that no logs were required for access to those vaults?

Mr. PODONSKY. I think there seems to be—I think it is safe to assume that they knew that, but I also think that it is clear from our going through the requirements that it is not clear throughout the Department and the security community of the Department as to what all the requirements are, because a lot of the requirements have not been memorialized in policies. A lot of them go back to memorandum, and that's why one of the recommendations in our report was to also memorialize these requirements into DOE orders.

Mr. BURR. If the chairman would allow me one last question, is it safe for this committee to assume that the security directives to these labs would be filtered from DOE headquarters to the DOE field office and then to the labs or is security a process that takes place only between headquarters and the labs themselves?

Mr. PODONSKY. It is supposed to work that they go—that it goes through the lines. So General—the policy arm under General Habiger would promulgate the policy and it would be implemented by the new NNSA, General Gordon, and he in turn would pass it down to the labs through the Albuquerque field office.

Mr. BURR. I thank you for that. I yield back, Mr. Chairman.

Mr. UPTON. Ms. DeGette.

Ms. DEGETTE. Thank you, Mr. Chairman. I apologize for my tardiness. I know Mr. Green and I at least, probably a few other members, are also downstairs at the YNY hearing. So thank you. And I hope I don't repeat anything, but thanks for having this hearing because I know a number of us at the last hearing thought it would be important to have this and I appreciate it. I think we should keep doing it until we hammer this thing out.

Mr. Podonsky, my first question, I guess, is that I was reading Dr. Browne's testimony and he says that almost all of Secretary Richardson's directives have now been instituted. You have been at the labs quite often in the last year. How many of these changes have you seen that have actually been instituted?

Mr. PODONSKY. Most recently at Los Alamos we were not allowed to come—prior to your attendance, I talked about the fact that the FBI investigation was still ongoing.

Ms. DEGETTE. Right.

Mr. PODONSKY. But for the most part what we have seen at Sandia and Livermore, in the last month, is that most all of the Secretary's initiatives have been, if not started, they are well underway.

Ms. DEGETTE. Do you know when they were started?

Mr. PODONSKY. No. I would have to go point by point to see which ones, but while we were at the site and—both sites, Sandia and Livermore, last month, when the Secretary's memo came out they immediately started initiating corrective action.

Ms. DEGETTE. So that was last month?

Mr. PODONSKY. June 19.

Ms. DEGETTE. And what about before June 19, do you know how many had been instituted?

Mr. PODONSKY. Everything that we have seen, when the Secretary first created our office to go out last—starting last May, everything that we saw promulgated from headquarters was at some stage being implemented.

Ms. DEGETTE. What about the integrated safeguards and security management system that's supposed to raise employees' security awareness levels? Have you looked at the implementation of that in any of the labs?

Mr. PODONSKY. We, before we were doing security, we looked at integrated safety—integrated safety management and the concept has resonated well enough throughout the Department that I know General Gordon and General Habiger have been talking about having the same concept of integrated security management.

Ms. DEGETTE. Right.

Mr. PODONSKY. It is still in the conceptual form. There is a lot of acceptance to that, but it has not been implemented.

Ms. DEGETTE. Do you know if there is a timeframe for implementation? Because I thought the standards had been agreed upon and that they were starting to implement it.

Mr. PODONSKY. I would have to defer to the second panel.

Ms. DEGETTE. Okay. So you don't know?

Mr. PODONSKY. No.

Ms. DEGETTE. The Rudman Report concludes that to have safe and successful security management systems mean that the security staff have a voice in every management decision and a voice equal to that of the program people. Is that model in the new management system that you know of?

Mr. PODONSKY. I am not aware of what it is comprised of.

Ms. DEGETTE. So you don't even know anything about the system?

Mr. PODONSKY. Not in its present state.

Ms. DEGETTE. Okay. Who would know about that?

Mr. PODONSKY. I think perhaps General Habiger or General Gioconda or perhaps even the lab directors might be able to address that.

Ms. DEGETTE. Mr. Wells, do you know anything about this system?

Mr. WELLS. At the request of this committee, we have been on the job a couple of weeks and we bought our airline tickets and we are heading out.

Ms. DEGETTE. So you haven't even——

Mr. WELLS. We will look at it.

Ms. DEGETTE. All right. Okay.

Now, Mr. Podonsky, back to you, over the years DOE has significantly relaxed its inventory controls over Secret and Top Secret documents in order to be consistent in the way that the Defense Department and other agencies handle this classified material.

As I looked at your testimony before I came in today, this change did not originate in the DOE but at the National Security Council in 1990. Can you explain why there had to be one industrial security standard? Where did the push for that come from?

Mr. PODONSKY. All I can tell you from my reading of the documents and my staff's reading of the documents was that President Bush asked the National Security Council to prepare a comprehensive review to explore the development of a single industrial security program and determine whether there could be cost-benefits of aligning the private sector with the government. It was in an effort, as far as we could tell, for both the cost savings and also to bring—to bring into control whether or not we protected all secrets and to, what we talked about, have a graded approach where those more sensitive documents or information were protected at the same standard.

Ms. DEGETTE. And I assume that some of that push or at least there was support from the industry, from the outside contractors who had to comply with various different standards; would that be accurate?

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

Ms. DEGETTE. Do you think here today that industrial security is as tight as national security should be? Is there accountability, do you think, for the most secret documents?

Mr. PODONSKY. Not for—when you look at the Department of Energy, the Department of Energy is unique in the type of information it has. So while we believe that there can be a more even playing field for industrial security for some of our resources, the most sensitive documents that are contained, and information contained in the Department, need to have a much higher standard.

Ms. DEGETTE. Now, what about documents that have been given up decades ago by the Defense Department? Where is the accountability for those? Do you know?

Mr. PODONSKY. I have no idea.

Ms. DEGETTE. Now, last September you wrote a memo to General Habiger telling him that the biggest security threat was from the active insider.

[The information referred to follows:]

September 3, 1999

MEMORANDUM FOR: Eugene E. Habiger, Director
Office of Security and Emergency Operations

FROM: Glenn S. Podonsky, OA-1

SUBJECT: Human Reliability Programs in the Department of Energy

During our recent meeting at Los Alamos you voiced a desire to take a harder look at the manner in which Human Reliability Programs (HRP) – specifically, the Personnel Security Assurance Program and the Personnel Assurance Program – are administered within the Department. We agree with you that a good Department-wide scrub of HRP administration and functioning will be useful in determining the levels of meticulousness rigor, and consistency with which the programs are currently being implemented. The results may yield valuable insight regarding any additional policy guidance needed to improve program effectiveness.

However, the most serious concern we have with these programs does not involve program administration, but rather the Department's policy that allows the programs to be used to fully mitigate the active insider threat. That concern is explained and discussed below. Any thorough look at the Department's HRPs should include a critical analysis of this issue and its implications concerning the protection of national security interests.

Current Departmental security policy allows protection programs to take inappropriate and unjustifiable credit for HRPs. Consequently, HRPs are used to mitigate (on paper) high and moderate risks when no empirical evidence exists to suggest that HRPs actually reduce those risks.

As you know the basic purpose of HRPs is to try to provide early detection of aberrant behaviors (or conditions that might result in aberrant behavior) which may indicate increased security risk, so that individuals exhibiting such behaviors can be removed from sensitive positions until such time as appropriate intervention can correct the unacceptable behavior and its causes. Specifically, these programs attempt to identify individuals with: psychiatric/behavioral problems; medical problems – especially those requiring certain types of medication; or drug or alcohol abuse problems. HRP programs are designed for this purpose only. Our experience shows us that at best, they will identify some portion of that small minority of program participants who manifest the types of symptoms or behaviors specified, and who may therefore potentially do harm as a result of their medical/psychiatric problems or addictions. These programs do not even attempt to address the insider who represents the greatest potential threat – the cool, calculating individual who is neither mentally ill nor addicted, but who, for whatever reason (ideology, greed, revenge, etc.), is willing to take actions that place national security interests (e.g., nuclear weapons, SNM, etc.) in jeopardy.

Current Departmental policy allows security planners, analysts, and managers to use participation in an HRP to mitigate an individual's potential actions from those of an active insider to those of a passive insider. The policy technically does not rely solely on the HRP; it allows that when other physical, administrative, and personnel security programs are in place and fully functional, any residual (e.g.,

23

active
insider) risk can be mitigated by participation in an approved HRP. In fact and in practice, the HRP is the trigger; participation in an HRP is the determining factor for whether an individual is considered a potential active or passive insider.

On the face of it, this policy is grossly inappropriate from a security standpoint. By no stretch of the imagination does any HRP provide a significant level of assurance that its participants do not pose an active insider threat – the programs are not designed for that purpose. The genesis of this policy is not completely clear, but may have been driven by two factors:

1. A belief (or agreement) that if the Department was going to require facilities to expend the effort and funds required to implement and administer HRP programs, then the facilities should be able to take some "credit" or see some "return" for that expense and effort.

2. The Department has been unable to devise an effective and acceptable solution to the insider problem. Effective prevention of unacceptable insider actions would probably require a significant additional investment in physical facilities/systems and/or rather stringent (some would say oppressive) internal security measures in the workplace – measures that may not be acceptable in our society. However, without somehow mitigating the active insider threat, it was impossible to reduce some moderate and high-risk scenarios to acceptable levels.

The HRP therefore became the "magic bullet" that allowed this real-world dilemma to be "solved" through policy rather than through actual security measures: facilities and field offices could – without formally accepting elevated risk – essentially disregard elevated risk scenarios involving active insiders by placing potential active insiders into an HRP. In our opinion, the current policy is based on expedience rather than logic or sound analysis, since, as explained above, HRPs do not, nor are they designed to provide the protection this policy credits to them.

You are absolutely correct in your conclusion that a critical and objective analysis of this program and related policies is warranted because it essentially allows the Department to ignore or hide elevated risk scenarios by administratively reducing risk levels, thereby inaccurately characterizing actual protection postures. The Department should deal with the active insider threat through tangible, effective security measures; alternatively, the appropriate Departmental managers should formally and knowingly accept the elevated risks attributable to active insiders. Currently, those managers may, in fact, be "accepting" those elevated risks without realizing it.

If you or your staff wish to discuss this further, please let us know.

/S/

Glenn S. Podonsky, Director
Office of Independent Oversight
and Performance Assurance

24

Ms. DEGETTE. You said there were not adequate steps to deal with the active insider, and I know this is a concern that a lot of people on this panel and other places have. What steps did you have in mind?

Mr. PODONSKY. Well, as General Habiger actually has already begun to take this—you are talking about the human reliability program, and what I can say in open session here is that they have already taken steps to combine some programs to further enhance the reliance on the human reliability program.

When you talk about threats in security, you talk about an external threat and you talk about an internal threat. An external threat is protected against various things such as barriers, a security force, fences, alarms, sensors. When you talk about internal, you talk about access controls, clearances. And as we have talked about before your arrival, one of the things that's vitally important to take into consideration is while there is never going to be an absolute there is going to be a reliance on the individual responsible for maintaining their security responsibilities.

A lot of these people that we are talking about, where there are violations, are actually creators of the information that we are talking about. So there is intellectual property that one needs to take into consideration as well. Our comment——

Ms. DEGETTE. Yes, but, you know, the guy who invented Coca-Cola was subject to company security policies that he not reveal that formula even though he thought of it.

Mr. PODONSKY. And for the most part, I believe that—I don't have the statistics but I would believe you would find that for the most part the Department has been—has a pretty good track record in terms of the individuals, now that notwithstanding the aberrations that we have seen over the last 14 months.

Ms. DEGETTE. Yes, but just to finish up, the problem is when you had the aberrations over the last 14 months that can undermine our national security network.

Mr. PODONSKY. And that——

Ms. DEGETTE. You have to set up a system, as you say, both external and internal, that's going to eliminate, as much as possible, chances for problems, because even one problem can be devastating.

Mr. PODONSKY. Correct, and that's why we wrote the letter to General Habiger to encourage them to take another look at their controls against the insider.

Ms. DEGETTE. Thank you, Mr. Chairman.

Mr. UPTON. Dr. Ganske.

Mr. GANSKE. I have here Executive Order 12958, dated April 17, 1995, signed by President Clinton. It deals with the classified national security information.

[The information referred to follows:]

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release April 17, 1995

EXECUTIVE ORDER 12958

- - - - - - -

CLASSIFIED NATIONAL SECURITY INFORMATION

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1 ORIGINAL CLASSIFICATION

Section 1.1. Definitions. For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the

United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be

expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. Classification Levels. (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) **Delegation of original classification authority.**

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. Classification Categories.

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States,

including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair the development or use of technology within a United States weapons system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;

(7) impair the ability of responsible United States Government officials to

protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. Identification and Markings. (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from declassification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives

issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. Classification Prohibitions and Limitations.

(a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2 DERIVATIVE CLASSIFICATION

Sec. 2.1. Definitions. For purposes of this order: (a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. Use of Derivative Classification. (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3 DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. Definitions. For purposes of this order: (a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. Transferred Information. (a) In the case of classified information transferred in conjunction with a transfer of functions, and

not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. Automatic Declassification. (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair

U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that

included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. Systematic Declassification Review. (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon

review.

(b) The Archivist of the shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6. Mandatory Declassification Review. (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise

and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless

such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. Declassification Database. (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4 SAFEGUARDING

Sec. 4.1. Definitions. For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. General Restrictions on Access. (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the

information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. Distribution Controls. (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. Special Access Programs. (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) Requirements and Limitations. (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each

agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. Access by Historical Researchers and Former Presidential Appointees. (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5 IMPLEMENTATION AND REVIEW

Sec. 5.1. Definitions. For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements

of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2. Program Direction. (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. Information Security Oversight Office. (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its

responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. Interagency Security Classification Appeals Panel. (a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as

the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) Rules and Procedures. The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5. Information Security Policy Advisory Council. (a) Establishment. There is established an Information Security Policy

Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) Functions. The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policiesestablished under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) Meetings. The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the

Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. General Responsibilities. Heads of agencies that originate or handle classified information shall: (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order; and

(c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly

involve the creation or handling of classified information;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

PART 6 GENERAL PROVISIONS

Sec. 6.1. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. Effective Date. This order shall become effective 180 days from the date of this order.

WILLIAM J. CLINTON

THE WHITE HOUSE,
April 17, 1995.

# # #

Mr. GANSKE. Now on page 3, there is something that bothers me a little bit because it says, for classification under section 1.3, that if there is any significant doubt about the appropriate level of classification it shall be classified at the lower level.

That bothers me a little bit. But as I have briefly perused this, you know, the closest I can come to the order for these changes that occurred with the requirements discontinued for various types of security arrangements, is on page 18, in which it says, each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

My question to you gentlemen is: No. 1, are you familiar with this Executive Order? And No. 2, am I missing something in this Executive Order?

I do not see in this Executive Order specifics for discontinuance of, let's say, approval for reproduction. I don't see specifics for discontinuance of Top Secret control officers. This is a much more general document.

Am I correct in reading this document?

Mr. PODONSKY. Yes, you are.

Mr. WELLS. Yes, you are.

Mr. FENZEL. Yes.

Mr. GANSKE. Okay. Well, I am getting kind of frustrated because I am trying to figure out who is responsible for these changes. Now this is a generalized Executive Order, so these types of specifics aren't in this Executive Order. Who specifically directed that, for instance, the approval for reproduction of documents, which was required in 1995, would be discontinued? Can you gentlemen tell me that?

Mr. FENZEL. My guess is DOE is responsible because in 1998 there was a——

Mr. GANSKE. Well, who in DOE gave that order and where is the paper order for that?

Mr. FENZEL. I don't know who signed. I don't know who signed. We can go back and look at the order, who actually signed it.

Mr. GANSKE. Would you please provide the committee with that information?

Mr. FENZEL. We can provide that.

[The following was received for the record:]

SIGNERS OF DOE ORDERS

DOE-5635.1A: Control of Classified Documents and Information, 2-12-88

Signer: Lawrence F. Davenport, Assistant Secretary, Management and Administration

Action: Initiated 100 percent inventory. Accountability over secret and top secret documents

Jan. 30, 1992, Memo: Change in Requirements for the Inventory of Classified Matter

Signer: Edward J. McCallum, Director, Office of Safeguards and Security, Office of Security Affairs

Action: Periodic inventories of classified matter below top secret will no longer be required when matter is maintained within a DOE-approved limited or exclusion area.

May 15, 1992, Memo: Accountability Requirements for Secret Documents

Signer: George L. McFadden, Director Office of Security Affairs

Action: Secret matter is removed from accountability if it is confined to a limited or exclusion area.

DOE 5635.1A Chg 1, Control of Classified Documents and Information, 6-14-93

Signer: Linda Sye, Acting Assistant Secretary for Human Resources and Administration

Action: Defines accountable matter as top secret matter and secret that is maintained outside of limited or exclusion areas.

DOE M 471.2-1A: Manual for Classified Matter Protection and Control, 1-9-98

Signer: Archer L. Durham, Assistant Secretary for Human Resources and Administration

Action: Defines accountable matter as top secret or secret mater stored outside of a limited area (or higher).

Mr. GANSKE. We need to find out who that individual is and we then need to ask that individual in a hearing who did he talk to about that.

I want to find out similar information, who was the individual in the Department of Energy that, for instance, discontinued the requirement on copy and series designation? Who changed the requirement on the Top Secret control officer, because then we need to ask that individual who did he talk to? Did he talk to the Secretary of the Department of Energy about that? Did the Secretary of Energy at that time talk to the President about that?

Look, I am getting tired of having these hearings and not finding out who is responsible for this.

You can't blame it on this Executive Order except in the generalized sense that it loosened—it allowed a loosening of these, but this Executive Order, as I read it, doesn't deal with this type of specifics.

So, gentlemen, I am asking you to provide to this committee, within the next week or 2, the information, the paperwork, from the Department of Energy on the specific memos that went out to these laboratories saying that these requirements which were in place in 1995 could be discontinued. Can you give our committee that kind of information?

Mr. WELLS. Yes, sir.

Mr. FENZEL. We should be able to.

Mr. GANSKE. Is it there? Do you know if that information is available?

Mr. PODONSKY. I can't speak for GAO but, yes, we do believe that there is a paper trail and we are still—we are still gathering that now for the Secretary.

Mr. GANSKE. How long will it take you to provide this committee with that information?

Mr. PODONSKY. We can do it within the week.

Mr. GANSKE. I thank you very much and that's all the questions I have.

Mr. STUPAK. Could you provide us a copy of the Executive Order you are speaking of?

Mr. GANSKE. Sure.

Mr. STUPAK. Thanks.

Mr. GANSKE. Thanks.

Mr. UPTON. Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman.

I guess my question will go to the Department of Energy, and I apologize if I seem to be approaching this from a simpleton ap-

proach. Right now we have an individual supervising a log system for access to the vault; is that what we have now?

Mr. PODONSKY. Yes.

Mr. BILBRAY. We reinstituted the log system?

Mr. PODONSKY. Yes, General Habiger did reinstitute that under the Secretary's direction.

Mr. BILBRAY. The log system is supervised by an individual who specifically checks identification and supervises the sign-in and sign-out process?

Mr. PODONSKY. That's what we understand. We have not gone back out to inspect to make sure that that is how it is being implemented.

Mr. BILBRAY. How long ago did we implement this?

Mr. PODONSKY. June 23.

Mr. BILBRAY. So we assumed it has been but in the last couple of weeks you haven't—no one has checked to make sure it is operating the way it was directed?

Mr. PODONSKY. No. Our oversight folks have not done that. Perhaps the policy group in the next panel could tell you whether they have actually done that.

Mr. BILBRAY. Okay. Do we have any electronic inventory tracking system on these documents?

Mr. PODONSKY. I am not aware that that is the case right now.

Mr. BILBRAY. Okay. Do we have any video surveillance systems on these documents or on the environs for access and egress?

Mr. PODONSKY. At some locations we might. I don't know across the board.

Mr. BILBRAY. Okay. So it seems like right now we are sort of operating under a 1941 model of a piece of paper, people sign in by a security person and sign out; basically a system that would have been right at home to our fathers during World War II and our mothers during World War II?

Mr. PODONSKY. And again, Congressman, there may be other pieces that are currently in place but the currency of my teams, we came back off the road on June 23.

Mr. BILBRAY. Okay. This change in the 1995—or the changes we have seen over the last few years, why were these changes made?

Mr. PODONSKY. I don't have a good answer for you because we asked the same questions.

Mr. BILBRAY. I will tell you something. What I am concerned about is that we can change systems, we can go through procedures. What I am really worried about is the institutional mindset of why were these changes made and who made them? What were they thinking? Is this an attitude that now that the so-called cold war is over that now don't worry about it? Was it sloppiness or was there a real intention on the fact that this is no longer—national security or national secrets are no longer a high priority?

I think the biggest question is not the institutional—I mean, not the structural system but the institutional mindset. Like I said before, I am really worried that this is being perceived as being a huge responsibility.

Mr. Wells, are we going to be looking at developing an internal system within our own government structure? Are we going to be looking at bringing the private sector into some called-for proposals

to see how we can upgrade this and make it a system that's more compatible with this millennium rather than 1941?

Mr. WELLS. Cyber technology is here today. We need to catch up quick in terms of what the requirements are.

Mr. BILBRAY. You know, I mean I know right now from maybe because San Diego is a high tech center that—I mean I have got companies that use a strip about the size of a hair on every one of their documents and anywhere that document moves anywhere in the building they know exactly when and where it was there. I am just wondering how are we going to gain access to what the private sector has been using for over a decade and use it for our most precious secrets? Is there any vehicle being considered to be able to go out and draw on these resources and have them participate in the development of the new upgraded security mode?

Mr. WELLS. Certainly I don't have an answer for you today but we will certainly pose that question to our audit teams and try to find out if there is something out there that would be applicable to be used under these circumstances.

[The following was received for the record:]

We are exploring that question as part of our ongoing work.

Mr. BILBRAY. I just hope those of us in government take advantage of this knowledge. And the way to do it is not to go out for bid, don't say what you want and how much it is going to cost but go out for proposals and say bring us the best packages you guys can develop so that you see exactly what's out there. I think the call for proposal is the only responsible way to go, but this is one member's opinion.

Thank you very much, Mr. Chairman, and I yield back.

Mr. UPTON. Mr. Cox.

Mr. COX. Thank you, Mr. Chairman. I thank our panel for being with us.

Two weeks ago, Congress received a report of the Redmond panel. Paul Redmond, of course, is well-known to you. He is one of America's leading counterintelligence experts and was the head of counterintelligence at the Central Intelligence Agency until recently.

Have you all read this Redmond Report, the unclassified or the classified version?

Mr. PODONSKY. No, I have not.

Mr. WELLS. No, I have not.

Mr. FENZEL. No, I have not.

Mr. COX. I would like to ask you some questions about it and so I will share it with you as part of the question so you at least have the relevant portion to which to respond.

Mr. STUPAK. Mr. Cox, I am sorry to interrupt, but do you plan on putting that in the record then so we all have it?

Mr. COX. Yes, we ought to add it to the record of this committee. It has already been put on the Union Calendar and introduced in the Committee of the Whole House.

Mr. STUPAK. Okay. None of us have it here.

Mr. COX. In fact, this is the House print of it. It is a House document and that is, of course, only the unclassified version of the re-

port. It is dated as entered into the record of the House June 21, 2000. But if the chairman agrees——

Mr. UPTON. Without objection it will be made a part of the record here.

[The information referred to follows:]

Union Calendar No. 386

106TH CONGRESS 2d Session	HOUSE OF REPRESENTATIVES	REPORT 106–687

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

REPORT

OF THE

REDMOND PANEL

IMPROVING COUNTERINTELLIGENCE CAPABILITIES AT THE DEPARTMENT OF ENERGY AND THE LOS ALAMOS, SANDIA, AND LAWRENCE LIVERMORE NATIONAL LABORATORIES

JUNE 21, 2000.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
79–006 WASHINGTON : 2000

LETTER OF TRANSMITTAL

PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC, June 21, 2000.

Hon. J. DENNIS HASTERT,
Speaker of the House,
U.S. Capitol, Washington, DC.

DEAR MR. SPEAKER: Pursuant to the Rules of the House, I am pleased to transmit herewith a report submitted to the Permanent Select Committee on Intelligence of the House of Representatives by a team of investigators headed by the renowned expert in counterintelligence matters, Mr. Paul Redmond. The document is styled, "Report of the Redmond Panel: Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories." The Committee by majority vote earlier today authorized the filing of the report for purposes of printing.

Sincerely yours,

PORTER J. GOSS,
Chairman.

Union Calendar No. 386

106TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 106–687

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE REPORT OF THE REDMOND PANEL "IMPROVING COUNTERINTELLIGENCE CAPABILITIES AT THE DEPARTMENT OF ENERGY AND THE LOS ALAMOS, SANDIA, AND LAWRENCE LIVERMORE NATIONAL LABORATORIES" FEBRUARY 2000

JUNE 21, 2000.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GOSS, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

EXECUTIVE SUMMARY

In the wake of last year's reports by the Cox Committee [1] on Chinese nuclear espionage and by the President's Foreign Intelligence Advisory Board (PFIAB) on security lapses at the Department of Energy's (DOE's) nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61 (PDD–61),[2] Secretary of Energy Bill Richardson embarked on a comprehensive reform of counterintelligence (CI) at DOE. This was accelerated and significantly refined in response to legislation proposed by Congress which, among other things, created the National Nuclear Security Agency (NNSA).

The House Permanent Select Committee on Intelligence established a bipartisan investigative team in the first quarter of FY 2000 to examine the Department of Energy's plan to improve its counterintelligence posture at its headquarters in Washington and its three key weapons laboratories. The purpose of the examination was to review the status of reforms and to examine issues still unresolved or under consideration. The team was comprised of a majority staff member, a minority staff member, and a special staff consultant, Mr. Paul Redmond, one of America's leading experts in

[1] The Cox Committee's formal name was the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China.

[2] PDD–61 was issued on February 11, 1998 in response to reports from the General Accounting Office and from the Intelligence Community that derided CI and security at DOE and its constituent laboratories.

79–006

CI and a former head of CI at the Central Intelligence Agency (CIA).

In general, the review determined that DOE has made a good but inconsistent start in improving its CI capabilities. The most progress has been made in building an operational CI capability to identify and neutralize insider penetrations. The two areas of greatest shortcoming, either of which could derail the whole CI program, are in CI awareness training and in gaining employee acceptance of the polygraph program.

Among the specific findings and recommendations from the review are:

- The current director of CI at DOE is an excellent choice for the job. Moreover, he has access to and the support of the Secretary.
- DOE has failed to gain even a modicum of acceptance of the polygraph program in the laboratories. DOE must involve laboratory management in deciding who will be polygraphed.
- DOE's efforts to improve CI awareness training have failed dismally. In developing its CI awareness training program, DOE should draw on the positive experience of other U.S. government agencies, in particular the CIA and National Security Agency (NSA).
- DOE also faces a considerable challenge in the area of cyber CI, that is, protecting classified and sensitive computerized media databases and communications from hostile penetration. This will require significant investment in defenses and countermeasures and require the assistance of other federal agencies.
- DOE CI has established an excellent, well-staffed, and effective annual CI inspection program that will serve to ensure the maintenance of CI standards and continued improvements in the program.
- The "shock therapy" of suspending the foreign visitor and assignment programs worked in making the laboratories realize the degree to which these programs, if not properly managed, can be a counterintelligence threat. The CI components at the laboratories now appear to be better involved in the process of granting approvals for visits and assignees.
- Cooperation at each laboratory between CI and security personnel is largely informal and dependent upon personal relationships. DOE and the laboratories must establish more formal mechanisms to ensure effective communication, coordination, and, most importantly, the sharing of information.
- The CI offices at the laboratories are hampered by their not being cleared for access to certain Special Access Programs (SAPs). Thus, the CI components are unable to exercise CI oversight of these activities. The Director of Central Intelligence (DCI) should work with the DOE Secretary to remedy this situation.
- DOE needs to establish contractual CI performance standards for the laboratories against which they can be judged and duly rewarded or penalized.
- It should be noted that the Committee has not adopted the Redmond Panel's position in favor of the maintenance of the

current centralization of all CI authority at DOE for a short, transitional period.

Introduction and scope of investigation

The scope of the team's investigation was to determine what has been done by the Department of Energy (DOE) and its key constituent nuclear weapons laboratories to improve counterintelligence (CI) policy and practices in the wake of the nuclear espionage investigation at Los Alamos National Laboratory. The team was limited to evaluating CI capabilities at the three principal nuclear weapons laboratories at Los Alamos, Sandia, and Lawrence Livermore, and at DOE Headquarters. The team was also to propose additional measures to improve CI at those facilities if, in the judgment of the team members, such measures were warranted.

The team interviewed DOE officials in Washington, D.C., California, and New Mexico. It also interviewed contractor employees of DOE, including employees of the University of California and Lockheed-Martin, at the three nuclear weapons laboratories. In addition, the team interviewed numerous officials of the Federal Bureau of Investigation (FBI), both at FBI Headquarters and at FBI Field Offices in San Francisco, California and Albuquerque, New Mexico, and officials of the Central Intelligence Agency (CIA) and the National Security Agency (NSA).

This report is not linked to DOE's own progress reports, which cite percentages of CI steps that DOE considers to be "implemented" at the three weapons laboratories. The team quickly determined that DOE used imprecise terms in describing the results of its self-evaluation. For example, the word "implemented" is commonly understood to mean that something has actually been accomplished, whereas DOE considers a CI directive as implemented when it has only been promulgated. For instance, in a September 1999 progress report, DOE claimed to have implemented the recommendation that lab CI offices contact all employees and contractors who have met with foreign nationals from sensitive countries. From its on-site visits the team determined that, although the laboratory CI offices are aware of the recommendation, they have yet to carry it out. The team thus does not believe that DOE's evaluative methodology is useful in assessing the true extent to which CI measures have been "implemented."

Historical comment: In the course of interviewing numerous laboratory personnel, the team encountered a pervasive, but muted, sentiment that many of the CI and security problems at the laboratories were exacerbated, if not caused, by the policies of former Energy Secretary Hazel O'Leary. These policies included the redesign of laboratory identification badges that resulted in the intentional obscuring of distinctions between clearance levels, the collocation of Q-cleared personnel with individuals who held lesser clearances, and the widespread use of "L" clearances—which still require only the most cursory background check for approval. One senior lab official opined that the L clearance program was "the worst idea in government—cursorily clearing people who didn't need access to Q material created new vulnerabilities."

The team notes that DOE was not unique in de-emphasizing basic security procedures in the wake of the end of the Cold War. The State Department, for example, embarked on its now infamous

"no escort" policy, the Defense Intelligence Agency issued "no escort" badges to Russian military intelligence officers, and even the Central Intelligence Agency precipitously abandoned its policy of aggressively recruiting Russian intelligence officers. The present and future Administrations must ensure that such laxity will never again be encouraged or tolerated.

DOE Office of Counterintelligence (DOE CI)

Presidential Decision Directive NSC 61 (PDD 61), issued on February 11, 1998, provided for the establishment of a new DOE CI program that reports directly to the Secretary of Energy. In April 1998, DOE's CI office became operational. Under the guidance of the director of DOE CI, Mr. Edward Curran, the Department has made considerable progress towards establishing an effective CI operational capability at DOE Headquarters to do the analytical and investigative work necessary to identify and neutralize insider penetrations. It is the team's opinion that Mr. Curran is ideal for the CI director job because of his extensive CI experience at the FBI, his rotational assignment at the CIA, and his persistence and determination.

Mr. Curran appears to have access to and the support of the Secretary of Energy, which is an essential ingredient to an effective CI program. Moreover, he is vigorously attempting to exert DOE CI authority and influence over the laboratories, which, while difficult to accomplish, is critical to the success of the new CI program. In the future, direct access to the Secretary and close working relations with other offices reporting directly to the Secretary, including the Offices of Security Affairs and Intelligence, will be crucial. In addition, DOE CI must establish and maintain a mutually supportive relationship with the Office of Independent Oversight and Performance Assurance, which performs inspections of DOE programs and policies. This office has an established record[3] of detecting, documenting and reporting CI and security shortcomings at the laboratories. Regrettably, past findings of this office in the CI realm evidently were rarely acted upon. This office, which is philosophically attuned to CI and security issues, now has a good working relationship with DOE CI and has recently pointed out at least one CI cyber security[4] vulnerability. In the future, the office will be a natural ally for DOE CI as it tries to assert authority, identify problems and implement new policies.

Mr. Curran is hiring and, where necessary, training a good cadre of CI officers to perform investigations from DOE Headquarters. The CI components at the laboratories,[5] moreover, seem well on the way towards adequate staffing. Laboratory interaction with the FBI appears to be effective, at both the management and CI component level. That said, laboratory CI offices will need to focus for the foreseeable future on (1) gaining the confidence of their laboratory colleagues; (2) crafting CI programs that fit the unique needs

[3] In 1994, this office discovered a serious vulnerability at Los Alamos—there was no technical or policy impediment to the transfer of classified data from a classified to an unclassified computer system. This finding was apparently duly documented and reported to the requisite DOE offices and to Congress. Disturbingly, no remedial action was taken.

[4] Cyber security is meant to encompass security for all computer systems at DOE and the laboratories.

[5] The term "laboratories" will hereinafter include Los Alamos, Sandia, and Lawrence Livermore National Laboratories only.

of each lab; and (3) conforming to DOE's requirements for more standardized approaches and procedures. The team appreciates that the job of reforming CI at DOE and the laboratories will require steadfast resolve on the part of Mr. Curran and his successors, continued support from the Secretary, and sustained resources from Congress.

Congressionally mandated reorganization of DOE

Mr. Curran believes that any authority he may have had in his new job as DOE's director of CI will be greatly diluted by the new structure established in the National Defense Authorization Act for Fiscal Year 2000. While the team will not attempt to evaluate the restructuring plan, Mr. Curran's views on the matter remain germane to the team's evaluation of how DOE Headquarters is approaching CI reform at the laboratories.

Mr. Curran indicated to the team that his initial plan had been to place federal employees rather than contractors as the CI chief at each laboratory. This would, in his view, create a more disciplined line of authority necessary to counter the historical unresponsivencss of the laboratories to DOE Headquarters directives. Mr. Curran ultimately accepted the argument put forth by the laboratories, however, that laboratory employees, i.e., contractors, would be more acceptable locally and would thus be more effective.

Mr. Curran believes that given the semi-autonomous status of new National Nuclear Security Agency (NNSA) under the statutory restructuring, he will have only a policy role and no actual authority over these contractors. In his January 1, 2000 implementation plan, the Secretary proposed that the present director of DOE CI serve concurrently both in that capacity and as Chief of Defense Nuclear CI in the NNSA.

Separation of CI and security disciplines at the laboratory level

The deliberate separation of CI and security disciplines at the laboratories, as advocated by DOE Headquarters senior management and as legislated by Congress could cause problems both at Headquarters and the laboratories. Management at each of the laboratories has sensibly placed CI and security where the expertise is. For instance, cyber security at all three laboratories resides under information management for organizational purposes. At Lawrence Livermore, the CI component resides under operations. Laboratory management and the CI chiefs appear satisfied with such arrangements. They uniformly indicated that security and CI are connected by what one Lawrence Livermore manager described as "multiple neurons" under such a rubric as an "Operational Security Group." This group ensures that each interested or responsible component is informed and involved as issues arise.

Such claims notwithstanding, the team discovered that these "multiple-neuron-type" arrangements are not formalized in any meaningful way at any of the three laboratories. In each case, the communications arrangements appear to depend primarily on personal and working level relationships. It has been the sad experience in many espionage cases that only after the spy is uncovered, does it become clear that a plethora of counterintelligence indicators concerning various facets of the individual's life, performance,

and behavior, had been known in different places by different individuals, but never effectively collated or holistically evaluated.

DOE must ensure that the CI officers at the laboratories are part of a formal system set up locally to ensure that all relevant CI and security data information is collected, assembled, and analyzed by means that are not solely dependent on personal relationships. Otherwise, the retirement or transfer of one individual in the process could cause the whole system to break down. Without an effective organizational structure, there is no guarantee that all relevant data will become known to the CI office. The team is not satisfied that DOE and the laboratories have completely grasped this concept. Moreover, the DOE Operational Field offices at Albuquerque and Oakland continue to refuse to share relevant information from employee personnel files under their control with DOE CI or laboratory CI components. The team learned that DOE CI is not even informed by these three offices when an employee loses his or her security clearance. Therefore, the team recommends that DOE ensure that a formal communications process for CI information between and within the laboratories and between DOE Operational Field offices and CI personnel be established immediately.

CI inspection teams

PDD–61 requires an annual inspection of DOE's CI program. DOE CI has hired and deployed a dozen retired FBI, CIA, and military intelligence officers to inspect the CI programs at the three weapons laboratories. This excellent initiative is already yielding promising results by identifying systemic problems and offering solutions. The inspection team consists of highly experienced individuals, who appear to be insulated from the politicization that can yield watered down findings. The team's effectiveness, however, will be largely dependent upon the frequency of its inspections. We recommend that DOE continue annual inspections as stipulated in PDD–61 and add follow-up inspections focusing on specific problem areas. The team judges that there is no DOE CI program that is more useful or efficient than this inspection regime. We recommend, therefore, that resources adequate to expand this inspection program be provided.

The inspectors have reasonably noted that since they are just beginning their program, they should focus on establishing a baseline for assessing where the laboratory CI programs should be within a year or so. The reaction at the laboratories to these inspections has been generally favorable, with only minor complaints about repetitious questioning and an over-reliance on the format of a standard FBI internal inspection that is not entirely appropriate for this effort. Some of the CI chiefs at the laboratories believe that the inspection teams, employing a narrow FBI focus, put too much emphasis on laboratory investigative capabilities and not enough on the information gathering, non-law enforcement role of the laboratory CI units. Also, the capability of the inspection teams in the difficult, arcane cyber area needs enhancement. Overall, however, this is a fine program. With some minor adjustments, it should become an effective instrument to ensure the continued improvement of CI at the laboratories.

Polygraph testing

Polygraph testing for "covered"[6] DOE and laboratory personnel was mandated by Congress, but DOE Headquarters reacted with poorly thought out and inconsistent directions to implement the requirement. As a result, laboratory personnel have a very negative attitude towards the polygraph. Moreover, since the polygraph is a highly visible part of the overall CI effort, the entire CI program has been negatively affected by this development. At the center of this problem is DOE's lack of success in explaining the importance and utility of the polygraph program. Further exacerbating this problem, DOE Headquarters personnel made little effort to consider the views of senior laboratory managers and have not involved them in the planning process for determining who will be polygraphed. In addition, DOE Headquarters efforts to meet with the laboratory employees to explain the polygraph program have been ineffective, if not counterproductive. To make matters even worse, DOE Headquarters, by vacillating and changing the policy over time, appeared inconsistent and unsure where the opposite is essential to instill confidence in the program parameters and professionalism.

The attitude toward polygraphs at the laboratories runs the gamut from cautiously and rationally negative to emotionally and irrationally negative. Moreover, the attitudes of the lab directors themselves range from acknowledgement of the need (although uncertain as to how to implement it), to frank and open opposition. Scientists at Sandia prepared a scientific paper purporting to debunk the polygraph for a laboratory director's use in a Congressional hearing. Employees at Lawrence Livermore wear buttons reading "JUST SAY NO TO THE POLYGRAPH." Other laboratory employees expressed the sentiment "You trusted me to win the Cold War, now you don't?" The team heard such statements as, "The Country needs us more than we need them" and "The stock options of Silicon Valley beckon." Several expressed a belief that many scientists will quit and that DOE will not be able to maintain the stockpile stewardship program. Still more employees cited an Executive Order that exempted Presidential appointee and "Schedule C" employees from having to take the polygraph as outrageous and unfair.

In addition to the emotional reactions, there are rational questions about the polygraph, such as, "What are they going to do with the inevitable number of people who do not pass?" The team shares this concern, and expects that there will be a significant number of so-called "false-positive" polygraph results that will have to be further examined. Another concern voiced to the team by numerous laboratory employees was that "No one has ever tried this before on this scale." The fact is that never before have so many "cleared" employees of a government organization had to have their clearances (and, thus, their livelihoods) threatened by the institution of the polygraph.

Compounding the problem further is an attitude among many laboratory employees that they are indispensable and special, and

[6] Section 3154 of the FY 2000 Defense Authorization Act defines "covered" persons as those involved in Special Access Programs, Personnel Security and Assurance Programs, Personnel Assurance Programs, and with access to Sensitive Compartmented Information.

thus, should be exempt from such demeaning and intrusive measures as the polygraph. Scientists do, in fact, represent a particular problem with regard to the administration of polygraphs. They are most comfortable when dealing with techniques that are scientifically precise and reliable. The polygraph, useful as it is as one of several tools in a CI regime, does not meet this standard. Accordingly, many scientists who have had no experience with it are skeptical of its utility.

DOE's efforts at explaining the utility of the polygraph as part of a multi-faceted CI program have been ineffectual. Moreover, DOE Headquarters' response to resistance at the laboratories, as unreasonable as that resistance may be, has been dictatorial and preemptory. As one senior DOE official observed, on hearing the complaint by the laboratories that the polygraph will make it difficult to recruit and retain top scientists, "It is already difficult to recruit and retain scientists in this economy, so what's the difference?"

In December 1999, the Secretary announced that DOE intends to reduce the number of employees subject to the polygraph to about eight hundred. This change, coupled with the elimination of the exclusion for senior political appointees, indicates that DOE Headquarters is trying to rectify the original overly broad and impractical scale of the polygraph program. Nonetheless, even this well-intentioned step has elicited skepticism. As one senior manager said, "What is to prevent some new Secretary from coming along and hitting us for not polygraphing all thirteen thousand laboratory employees?"

The team judges that DOE Headquarters should do more to involve laboratory management in the process of selecting those individuals to be polygraphed. Senior laboratory managers know what secrets need protecting and, thus, could bring their knowledge to bear on this process. Including managers visibly will involve them with the program in the eyes of the workforce. This will both motivate and enable them to sell the program, and, one hopes, give the program more credibility. Their participation, moreover, would make them accountable.

To this end, DOE must reinvigorate and revamp its effort to educate the workforce on how polygraphs, while not definitive in their results, are of significant utility in a broader comprehensive CI program. The polygraph is an essential element of the CI program and it will not work until it is accepted by those who are subject to it.

Counterintelligence awareness training

There has been no discernable, effective effort from DOE Headquarters to establish and support an effective CI training and awareness program. Moreover, the team was unable to identify any real efforts on the part of DOE CI to improve upon existing DOE training and awareness practices for laboratory employees.

No organization, governmental or private, can have effective CI without active, visible, and sustained support from management and active "buy-in" by the employees. It is not possible to do CI by diktat, or from a distance. In the words of one DOE officer, the CI program cannot be a success unless each employee "knows the requirements [of the program], his or her own responsibilities, and is trained to carry them out."

Historically, the laboratories have—on their own initiative—sponsored CI and security lectures and briefings to supplement the annual security refresher required of each employee. The CI lecture series at Lawrence Livermore is an excellent program. Unfortunately, it has not been replicated by the CI offices at Sandia or Los Alamos, which instead sporadically arrange ad hoc presentations.

Moreover, the annual security refresher, which these lectures supplement, is perfunctory and pro forma. It can consist of as little as a brief presentation on a personal computer followed by a short quiz to ensure that the employee has read the material. As a result, the refresher process is not taken seriously by the employees, especially since DOE Headquarters has dictated much of the content in the past without consulting the laboratories. The sample training materials examined by the team were bureaucratic, boring, turgid, and completely insufficient.

The poor state of the training program is also reflected in the mistaken belief by CI officials in Washington that a training facility at Kirtland Air Force Base in Albuquerque, New Mexico, is assisting in developing CI teaching materials for DOE's next annual refresher. When contacted by the team, the facility indicated that it was playing no such role. Clearly, DOE CI has yet to turn its attention to improving CI training.

In lieu of a department-wide program, the laboratories have taken some uncoordinated initiatives to meet some of their awareness training requirements, if only in response to the uproar caused by events at Los Alamos. Management at all three laboratories appears to have given some thought, at least, to what may be required. Managers have drawn an analogy between their successful occupational safety training and awareness program and how they are to make security and CI an accountable, integral part of each employee's daily work and professional mindset. At Sandia and Los Alamos, specifically, management recognizes that, as in safety management, it should give line managers specific roles and responsibilities for CI and security, and then hold them accountable. This would appear to be a constructive step.

THE VIEW FROM THE LABORATORIES

Laboratory management made the following comments regarding training and awareness:

- "Some of the awareness training material received from Washington is so bad it is embarrassing. Were it used, it would undermine the credibility of the whole program."
- "We had to scramble to find speakers on the subject [of CI during a lab-wide CI and security stand-down]."
- "One [CI] lecture given by an experienced former FBI agent, tailored to the laboratory audience, was a huge success. We need more of this sort of thing."
- "There is no line budget item for training, each speaker costs about $4,000, yet there is no Headquarters-generated program."
- "DOE Headquarters' approach to training and awareness has been form over substance, represented by dictated programs and policies."

- "There is an acute need for 'realistic' awareness training, so people will realize the problem did not go away with the Cold War and they are still targets."
- "There are [laboratory] divisions standing in line for tailored presentations."
- "Concrete examples, real [CI] incidents, and their consequences are required to get people's attention. They [the scientists] must be captured intellectually."

In the spring of 1999, the Secretary issued a series of short-notice security, CI, and cyber-related "stand-downs" at the laboratories. This was not well received by laboratory employees. Some characterized the stand-downs as a "frog marching exercise" that discredited the whole effort at improving CI by alienating significant parts of the workforce. An exception to this belief was at Los Alamos, where the stand-downs were viewed as a "unifying" experience—presumably because of the siege mentality that existed there in the wake of the nuclear espionage allegations.

The CI component at DOE Headquarters has a new training officer, and the office apparently intends to develop a program to support CI awareness and training at the laboratories. One starting point would be to follow the example of other successful CI training programs. CIA, in the aftermath of the Aldrich Ames espionage case, also instituted a very aggressive CI course and lecture program supplemented by an in-house television series. In addition, NSA has a long-standing, effective training and awareness program that the team examined at length prior to its field visits to the laboratories.

It is instructive to consider the experiences of NSA, particularly in dealing with the parts of NSA populated with an accomplished collection of world-class mathematicians and cryptologists. This highly skilled workforce is very similar to that found at the laboratories. The key factor in NSA's success in the training and awareness area appears to be that its overall integrated security and CI program has been in existence for many years, and the mathematicians enter a culture where, from the very beginning of their employment, security, CI, and the polygraph are "givens" in their daily work. DOE is now starting virtually from scratch and would do well to learn from the positive experiences of agencies such as NSA.

NSA has also had success with a program designating a security and CI referent for each significant component. This individual is not a security professional, but a regular employee of the component, one of whose additional duties involves dealing with security/CI issues. The referent, who receives some extra security and CI training, is partly rated on his performance in this role and is responsible for selling the CI program at the lowest bureaucratic level. This system, by all accounts, has been quite successful. Los Alamos has a large number of employees who are responsible for "security" in their units. Their role at Los Alamos could be expanded along the lines of the NSA model and could be adapted elsewhere. The team also notes that when it raised NSA's security/CI referent concept at each laboratory, there was widespread interest in it. Resources to enable the laboratories to institute a referent program along the lines of the NSA model should be provided.

DOE Headquarters must do much more to support field training and awareness by establishing a comprehensive curriculum for use by the laboratories that is interesting and substantive enough to catch the attention of the difficult laboratory audience, and sufficiently flexible to allow individual CI directors to address the specific needs of each laboratory. In addition, DOE should establish a CI training course for managers. Like the successful occupational safety management training, this course should emphasize that CI is an integral part of each manager's job.

Finally, Congress should support extensive CI training and awareness programs at DOE Headquarters and the laboratories. This should include providing funds specifically for this purpose in FY 2001 to ensure that training and awareness needs are met and that money is not diverted to other programs. Congress should carefully oversee the implementation of the program it funds to ensure that training and awareness becomes, and remains, a high priority for DOE.

Cyber CI

DOE and the weapons laboratories face their biggest challenge in the area of cyber CI. The magnitude of the problem and the complexities of the issues are daunting. There are several thousand systems administrators at the laboratories who have very wide access. There are each day hundreds of thousands of internal e-mails at the laboratories and tens of thousands sent to external addresses. Additionally, there are extremely complicated issues of connectivity and systems architecture. The laboratories, wherein reside massive brainpower and experience in cyber matters, are beginning to address this challenge cooperatively and, in some cases, with the assistance of other U.S. Government agencies. Some laboratories have in place programs using "key words" to scan e-mail traffic for CI indicators, but it is too early to formulate any substantive judgments of their effectiveness.

It is clear that DOE CI has not yet fully established its authority at DOE Headquarters and at the laboratories in the cyber area. The cyber component of DOE CI is trying to overcome legal obstacles centering largely on privacy issues related to the implementation of a pilot program to determine the size and difficulty of e-mail monitoring using sophisticated "visualization" software. There is another pilot program under development to detect cyber intrusions better. DOE CI is encountering bureaucratic resistance to establishing acceptable minimum standards. For instance, the laboratories are pressing for standards that are acceptable in a more open "academic" environment. Furthermore, a comprehensive intrusion incident reporting mechanism for the computer systems controlled by DOE information management offices and the laboratories is meeting resistance from DOE and laboratory personnel, who cite excessive reporting burdens.

There has existed for years at the laboratories an entity called the Computer Incident Advisory Capability (CIAC) that was responsible for collecting and analyzing computer security incident data. The reporting to this organization has historically been voluntary, and anonymity was permitted to encourage the laboratories to be frank and forthcoming. More recently, the CIAC has begun to provide DOE Headquarters with intrusion incident summaries.

The lack of specificity in these summaries, however, makes meaningful analysis impossible. DOE CI, with assistance and support from DOE management, needs to assert its authority in this matter.

It appears that DOE CI is very well served by employing detailees from the FBI and NSA. These detailees bring a high-level of expertise to the issue and some independence from DOE's bureaucracy. The practice of assigning them to play a leading role in the cyber CI component should be continued.

The DOE CI component believes that it has an effective working relationship with DOE's Office of Independent Oversight and Performance Assurance. This office conducts "red team attacks" on the computer systems and has helped impose computer security standards at the laboratories. Clearly, the functions of DOE CI and this office are complementary, particularly in the cyber area. This close working relationship will be a key to improving overall cyber CI.

In sum, DOE CI, faces in the cyber area, the same very difficult, complicated issues faced everywhere in the national security community. The individuals who create and run computer systems are, by training and motivation, inclined to promote the widest, fastest, most efficient dissemination and transmission of data; hence, the basic and pervasive mutual aversion between "Chief Information Officers" and the security/CI offices. The team believes that adequate resources should be provided for cyber security and CI, and that aggressive oversight should be exercised to ensure that effective programs are developed and implemented.

Foreign visits and assignments

The team limited its examination of this issue to the role played by DOE CI and the laboratory CI offices in the visitor and assignments approval process, which would lead to the laboratory director seeking a "waiver" to the moratorium on foreign visits from sensitive countries. The team notes that Secretary Richardson announced in December 1999 that he might start seeking such waivers as permitted by the FY 2000 National Defense Authorization Act.[7] All three laboratory CI chiefs stated that they now have an established, integrated role in the approval process leading to a laboratory director seeking a waiver to allow such a visit. For instance, the CI chief at Lawrence Livermore is one of four officers who must sign off before a request goes to the laboratory director for a decision to seek a waiver. The CI chief at Sandia is a member of the Foreign Visits and Assignments Team, which actually controls the approval process. These officials can thus bring to bear a CI perspective on any proposed visit, which the team believes to be a crucial function.

Obviously, the judgments made by the laboratory CI offices are only as good as data on which they are based. These data includes indices checks, which have often been slow in coming from other Federal agencies. The laboratory CI offices need to have access to broader-based intelligence information. This information, when integrated by the analysts in the CI offices, would give them a much improved basis on which to judge the CI threat that individual visitors and delegations might pose. Access to this information is prob-

[7] Washington Post, December 3, 1999 "Energy Chief to Allow Foreign Scientist to Visit Labs."

lematic, and DOE CI needs to work with other relevant entities at DOE Headquarters—particularly the Office of Intelligence—to arrange appropriate and efficient access in the field.

In addition, there are two relevant databases. The Foreign Assignments Records Management System (FARMS) is unclassified and is maintained by DOE security. The Counterintelligence Analytical Research Data System (CARDS) is maintained by DOE CI and is an outstanding repository of classified data on prospective foreign visitors. Laboratory CI offices believe that they need a "bridge" between these databases so they can more effectively use the information they contain. In addition, it appears that the laboratories, which in some cases maintained their own databases, feel less confidence in the quality of DOE-maintained data, and their access has become more cumbersome. DOE CI needs to address these problems.

Apparently, the legislatively imposed moratorium on foreign visits and assignment has had the desired effect of making DOE and the laboratories much more conscious of the CI threat posed by visits.[8] Making the laboratory directors accountable has also had a salutary effect. It now remains for DOE CI and the laboratory CI offices to work together to make sure the CI role in the approval process is made as effective as possible by bringing to bear the maximum amount of data as efficiently as possible. There will also need to be more awareness training to sustain and better improve the presently enhanced levels of interest and attention.

CI knowledge of special access programs (SAPs) and other sensitive projects

The laboratories do a considerable amount of work for the Intelligence Community under the auspices of the "Work-for-Others" program. This work, administered by DOE, is often highly sensitive and is administratively compartmented within SAPs, which require additional clearances. The laboratory employees who work on these SAPs or other projects technically fall under the CI jurisdiction of the laboratory CI office. The team discovered inconsistencies in this arrangement in two of the laboratories that could lead to potentially dangerous outcomes for CI if not corrected.

At Lawrence Livermore, laboratory CI officials are not permitted to become involved in the "Work-for-Others" programs involving Intelligence Community SAPs. They are not substantively or administratively informed of any aspect of the programs. Given that one of the primary functions of the laboratory CI staff is to brief employees on CI threats and to inquire about CI incidents, the CI office at Lawrence Livermore is unable to perform fully this critically important function. Lawrence Livermore's CI chief advised that he learns of "Work for Others" activities only "by mistake" or "by accident." In some instances when he has tried to involve himself in issues related to "Work-for-Others" activities, he has been restrained by his senior management, which presumably is seeking to enforce Intelligence Community requirements. A similar situa-

[8] Evaluating the security aspects of the visits and assignments program is beyond the team's remit and is therefore not addressed herein.

tion prevails at Sandia, where it was evident that the CI component is often unaware of "Work-for-Others" activities.[9]

The net result of this situation at Lawrence Livermore and Sandia is that no one appears to be examining CI issues involving personnel engaged in the most sensitive SAPs and other Intelligence Community projects without a formalized reporting mechanism, there is no guarantee that an employee will report a CI incident to the contracting intelligence agency. The contracting agency, may or may not, in turn, report the problem or issue to the DOE Office of Intelligence, DOE CI, or to FBI Headquarters. The team judges this to be an unacceptable process for the transmission of such critical CI information. DOE Headquarters should reach a formal agreement with the Intelligence Community to ensure that the laboratory CI offices are read into the SAPs at least at an administrative level so they can fulfill their CI responsibilities. The team also encourages the Community Management Staff (CMS), which has been tasked by the Director of Central Intelligence (DCI) to examine the protection of Intelligence Community equities by DOE and the laboratories, to work closely with DOE to resolve this issue of the lack of a formalized reporting mechanism.

Sensitive unclassified technical information (SUTI)

DOE has instituted a new pseudo-classification for material that is deemed sensitive, but is technically unclassified. The team encountered significant confusion at the laboratories about what will actually be captured under the SUTI category, and laboratory managers expressed strong opposition to the whole concept. One principal argument was that scientists who work at the laboratories are already precluded from publishing much of their work because it is classified. The scientists often feel that much of what they must treat as classified is actually publicly available and being discussed by their non-U.S. government peers around the world. Also, given that their scientific reputations are largely dependent upon what they publish and upon their interactions with their non-U.S. government peers, they feel that the SUTI category further prejudices their ability to earn scientific recognition. Moreover, laboratory employees pointed out to the team that the SUTI category is highly subjective, cannot be standardized in any fair way, and will necessarily compel them to look for work outside of government if it is strictly imposed.

It appears that the DOE Headquarters policy on SUTI is evolving much like its policy on the polygraph, with similar misinformation, misunderstanding, and general confusion among those who will be affected by it. At Los Alamos, senior managers advised the team that SUTI was no longer an issue because it had been replaced with a DOE list of sensitive subjects. It is interesting that Lawrence Livermore and Sandia were, at the same time, still laboring under the assumption that they would be subject to SUTI and were making decisions based upon this assumption.

In the team's judgment, DOE should proceed very cautiously and openly on SUTI imposition—if it does so at all—so as to avoid repeating the internal public relations mistakes it made with the

[9] Due to the communications arrangements between Los Alamos chiefs of intelligence, CI, and security, Los Alamos does not appear to have the same problem as the other two laboratories.

polygraph program. Moreover, it appears DOE has yet to address the significant legal implications associated with the promulgation and implementation of SUTI. This fact was acknowledged recently by DOE's General Counsel, who issued a notice stating that since "sensitive information" is neither defined in the National Defense Authorization Act for FY 2000, nor in DOE's existing regulations, DOE will not impose new statutory penalties associated with mishandling sensitive unclassified information. Therefore, until a clear and well thought out rationale and implementation plan has been formulated by DOE for SUTI—which must include engagement with laboratory management and personnel to be effective—the team believes that steps to implement SUTI regulations should not proceed.

Enforcement

Each contract DOE has with the operators of the laboratories requires an annual appraisal of performance. In the past, these appraisals apparently included an ineffective pro forma consideration of security. It appears that neither DOE Headquarters nor DOE Field Offices, which are directly responsible for contract oversight, effectively enforced the terms of the contracts in this area. For example, the team was told that in some instances the University of California was not consciously aware of the fact that it was contractually responsible for certain security provisions, even though these were explicitly stated in the contract. The team recommends that DOE enforce existing security performance measures. Further, the team recommends that DOE incorporate measurable CI objectives and performance standards into each of its laboratory contracts. DOE could then use the previously mentioned CI audits, possibly combined with the findings of the Office of Independent Oversight and Performance Assurance, to evaluate the performance of the laboratories and impose penalties on the contractors for unacceptable performance.

The team understands that DOE is working on language for contracts that will allow DOE to assess CI performance at the laboratories. The initiative represents an incentive for the laboratories to perform, and an opportunity to put in place measures to remedy past poor performance by the laboratories in this area. The team believes that Congress should support, encourage, and oversee the initiative, and ensure that DOE rigorously enforces the CI standards that it sets out in its contracts.

Conclusions

Hostile intelligence threats to DOE and the laboratories will most likely come from problems with trusted employees, cyber penetrations, and visitors or assignees. DOE has made good progress toward establishing effective operational mechanisms to cope with the problems of identifying possible "insider" penetrations and of laying the groundwork for the FBI to investigate. DOE has also set up an excellent inspection system to ensure the continued efficacy of these mechanisms, but it is not yet clear that this system is being evenly applied across all CI and security programs.

DOE has not effectively laid the groundwork for acceptance of the polygraph program, an obviously essential part of any CI effort to detect and deter espionage by employees. Moreover, DOE has

failed to establish the absolutely key, complementary CI pillar—an effective training and awareness program.

No CI program can succeed unless both the operational and training pillars are in place and supporting each other. Further, it is clear from decades of behavior, that the DOE and laboratory culture is profoundly antithetical toward CI and security. Unless changed, this entrenched attitude will doom any attempts at long-term improvements. Effective training and awareness programs are the only way to change this culture.

DOE is just beginning to determine the magnitude of CI issues relating to the cyber threat, which includes e-mail and intrusions. The cyber component of DOE CI needs strong support at DOE Headquarters to establish suitable, minimum CI standards in systems controlled by DOE's information management units and the laboratories.

Processes are now in place that should ensure that CI concerns will be factored into the waiver approval system for foreign visitors and assignments, questions of security in the approval process, however, were beyond the scope of this study.

In spite of progress in some areas, statements from DOE Headquarters, to the effect that all is now well in the CI area are nonsense. Problems and deficiencies caused by decades of nonfeasance and neglect cannot be fixed overnight. Such statements serve only to strengthen the position of those at the laboratories who would wait out the effort to improve CI and thus make the job all that much harder. Our yardstick for assessing the CI program will be their future success in catching spies.

○

Mr. COX. It will also be included in the record of this committee, as well it should be because it is precisely the same topic and a great deal of work went into the preparation of this report.

The Redmond Report finds two areas of greatest shortcoming. The first is gaining employee acceptance of the polygraph program and the second is counterintelligence awareness training. With respect to the polygraph program, this is as of 2 weeks ago, the report states, the Department of Energy has failed to gain even a modicum of acceptance of the polygraph program in the laboratories.

With respect to counterintelligence, it states, the Department of Energy's efforts to improve CI awareness training have failed dismally.

Mr. Podonsky, do you share that evaluation?

Mr. PODONSKY. I have no information to conclude that that is accurate. The information that I have is that there has been polygraphs being administered at the national labs, as well as other organizations such as my own and General Habiger's. But whether or not the counterintelligence program is effective or being accepted or whether the polygraphs are being accepted, I have no information.

Mr. COX. The reason that the Redmond Report is concerned with the lack of acceptance of polygraphs at the laboratories is the lack of implementation. Can you tell us how many people at Los Alamos, how many people at Livermore, how many people at Sandia, have been polygraphed?

Mr. PODONSKY. I can only ask you to defer that question to the second panel.

Mr. COX. Do you have a rough idea?

Mr. PODONSKY. Just ballpark numbers which I wouldn't want to quote because they are fourth party.

Mr. COX. Well, the answer is not very many and we can go into that with the next panel, but this program of polygraphing sensitive employees in the most sensitive nuclear weapons security positions is incipient. It is barely beginning and there has been a great deal of temporizing and, according to the Redmond Report, worse than that in putting the program into place.

Let me share with you more of what he has to say and what the panel has to say. First, the panel notes that Congress has mandated these polygraphs and also the President of the United States in President Decision Directive 61, which was issued in February 1998. So even a few months before the Congress created the Select Committee that issued its report on counterintelligence and security at the national weapons laboratories, the President of the United States had issued a direct order to the Secretary of Energy to implement polygraphing at the national laboratories.

That polygraphing, until very recently, had not even commenced and now it has barely commenced.

The Redmond Report further states with respect to this that Department of Energy headquarters personnel have made little effort to consider the views of senior laboratory managers and have not involved them in the planning process for determining who will be polygraphed. I can say that the chairman of this subcommittee, Mr.

Burr and myself found this also to be true on our field visits to the labs as members of this subcommittee.

The Department of Energy headquarters' efforts to meet with the laboratory employees to explain the polygraph program have been ineffective, if not counterproductive. To make matters even worse, DOE headquarters, by vacillating and changing the policy over time, appeared inconsistent, and I am sure where the opposite is essential, to instill confidence in the program parameters and professionalism. And the authors of this report saw the same thing that the subcommittee members did when they went to visits the labs. The scientists are wearing buttons that say "Just say no to polygraphs." Now these, of course, are employees of the University of California, contractors to the Department of Energy, in cleared positions.

Why is it that there is a direct order from the President of the United States that this program go forward, a direct legislative mandate from Congress and we can have a report in June of 2000 that tells us that the Department of Energy not only isn't doing it properly but is getting in the way?

Mr. PODONSKY. Congressman, I am not about to sit here and give you answers to information I know nothing about. I would only, again, defer to those who have been involved, Ed Kern and General Habiger.

Mr. COX. Mr. Wells, do you care to comment?

Mr. WELLS. Mr. Cox, to my knowledge we don't have any ongoing work involving that issue.

Mr. COX. Do you, Mr. Podonsky, think that polygraphing is an important part of security at the labs, and counterintelligence?

Mr. PODONSKY. I can only give you my personal opinion in doing oversight in this Department for quite some time and I think if polygraphs are administered in a reasonable fashion, that it can be—it can be employed to be useful. That's a personal opinion.

Mr. COX. Okay. Are you aware that at the labs, one of the complaints of the scientists was that President Clinton had issued an Executive Order that had exempted from polygraphs political appointees and Schedule C appointees?

Mr. PODONSKY. I wasn't aware of that, no, sir.

Mr. COX. The, I think, diplomatic statement in the Redmond panel about the ineffective, if not counterproductive, efforts of DOE headquarters in meeting with the scientists refers to the sensitivity sessions that have been held about polygraphs that have really made the problems worse in full public view.

I will say, if the chairman will permit, that when we have scientists at the labs responsible for very sensitive military secrets and we entrust them with this responsibility we also have to entrust them with enough information so that they can understand why they are being asked to change their behavior. And there is more information being shared in court these days with Federal judges than is being shared with our scientists. We have got to, as this report states, deal much more effectively with that problem. And the rest of these things that we are talking about here today, it seems to me, are symptomatic virtually so of this underlying problem.

The counterintelligence issues, I don't know whether my time has expired and I can come back to this.

Mr. UPTON. Your time has expired some time ago, but you can get more. I will allow you to have another round.

Mr. COX. I think we ought to do that because the counterintelligence issue, which the Redmond panel raises, is equally important.

I thank the chairman.

Mr. UPTON. And I might ask if we could retrieve temporarily your copy of the Redmond Report so we can make copies for the minority as well.

Mr. COX. Sure.

Mr. UPTON. Temporarily. We will get the copies back to you. Thank you.

Mrs. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. Podonsky, I may be asking a question that Mr. Burr may have covered before I came, but I would like to hear your answer to it. In your report, you refer to a request—which I believe is on page 19 of your redacted report—that early last year the weapons labs proposed to Under Secretary Moniz, that tighter controls be reinstituted for certain sensitive matter, including things like hard drives.

Do you know what happened to that recommendation?

Mr. PODONSKY. At the time of our special review out at Sandia, the staff at Sandia provided that fax to us. That was the first time that we had seen it, and specifically we don't know what happened after that was sent to Washington.

Mrs. WILSON. You say at the time of your review at Sandia. Which review would that be?

Mr. PODONSKY. Over Father's Day, the June 19 timeframe.

Mrs. WILSON. So that was after the problem at Los Alamos?

Mr. PODONSKY. Yes, ma'am.

Mrs. WILSON. So you had no knowledge of a recommendation to tighten security procedures before that?

Mr. PODONSKY. We had no knowledge of this memorandum or fax from the laboratory directors.

Mrs. WILSON. Would it be unusual for you to be excluded from the staffing of that kind of recommendation?

Mr. PODONSKY. No, not unusual at all.

Mrs. WILSON. Who in the Department of Energy would be involved in the staffing of that kind of recommendation? I am assuming that, you know, you can't expect the deputy to be seeing everything. What organization would that normally be routed to?

Mr. PODONSKY. That would be routed to the line responsibility, so that would be perhaps General Gioconda's organization, as well as the policy group for security, which would be under General Habiger.

Mrs. WILSON. Are you familiar with a program called ISecM that was instituted last year with respect to cyber security?

Mr. PODONSKY. My cyber security people are very familiar with that.

Mrs. WILSON. As I understand it, it was a response to the Wen Ho Lee incident, to try to deal with the insider security problem. Do you know what the cost estimate was to implement ISecM?

Mr. PODONSKY. No, ma'am, I do not.

Mrs. WILSON. Who in the Department of Energy would have that information?

Mr. PODONSKY. If I'm not mistaken, that originated out of the defense organization program so perhaps General Gioconda might have that information.

Mrs. WILSON. Thank you, Mr. Chairman. I yield my time.

Mr. UPTON. Thank you. For those members wishing another round of questions, I am going to pass and yield to Mr. Burr.

Do you have additional questions?

Mr. BURR. I do. I thank the chairman.

Let me follow up with where Ms. Wilson was. If I understood you correctly, you have the responsibilities for independent oversight?

Mr. PODONSKY. Yes, sir.

Mr. BURR. You said that it is not unusual for you to be excluded from requests about security upgrades from the laboratories?

Mr. PODONSKY. That's correct. And—I am sorry.

Mr. BURR. No, I am somewhat baffled by that as to how you could be excluded from the—given that you are responsible to do evaluations. I mean, we have had you do numerous ones, or DOE certainly has—that a document like that and a request from the directors of these labs might not have been supplied for you, as you evaluated what the current and—for your own recommendations, what they felt. That's accurate?

Mr. PODONSKY. That is accurate. I really—we don't find that terribly unusual from the standpoint of we do not manage any of the sites. We do not have responsibility that the line has, so I would not expect that we would be exposed to a lot of decisions that are made in the security arena that involve either policy, upgrades——

Mr. BURR. But it is clearly helpful to committees like this that are trying to look at the process that your report include, this is a deficiency; the directors of these labs have made a recommendation. I can't imagine that the Department of Energy would let you go through a review process and not make available anything that they felt was pertinent, or anything that was pertinent; but it is not unusual?

Mr. PODONSKY. No, and I would agree with your—with your statement that if—we should be exposed to a lot of the background of how decisions arise, but as those decisions are underway I don't find that to be unusual.

Mr. BURR. Let me read some of Mr. Browne's testimony because we won't have an opportunity to have you back up, and just get some comments on it.

"There are a number of special programs at Los Alamos in which line managers have little or no access to ensure that laboratory safety and security rules are met."

"Prior to this incident, it was not clear to our line management and security people whether or not they had the necessary authority to accept responsibility for the detailed security procedures of these programs."

They are referring to SAP and—nonSAP and nonSCI programs.

Is that inconsistent or consistent with your findings?

Mr. PODONSKY. From our past inspections, that is not consistent. We have found that the folks that in last year's inspection that we interviewed and looked at their programs, that they seemed to understand what their responsibilities were.

Mr. BURR. He goes on as it relates to the NEST program: "The NEST program has been operated as a closely held need-to-know program but not a formal special access program. Los Alamos has made a good faith effort to participate in this program, as we understood the guidance of the program sponsors in DOE. Oversight of NEST by our security division was limited. Not all aspects of the NEST security plan were reviewed and approved by laboratory managers for compliance with DOE rules or for best security practices. Even if NEST was treated as closely held need-to-know programs, it was subject to DOE policy for handling SRD and that policy was in place at the laboratory."

Can you comment on that statement by Mr. Browne?

Mr. PODONSKY. We believe that security at a site is the responsibility of the site and it is a shared responsibility with the DOE headquarters and the line organization. Specifically on NEST, we do know, as I mentioned, that we are going to do an inspection of all the NEST activities. We have not inspected the entire NEST activities since 1992, but looking at NEST as a program, we do know that there has been—prior to this past year and a half, there has been some confusion as to where the responsibilities and accountability for NEST lie.

Mr. BURR. Clarified in a memo several weeks ago by one of the Under Secretaries to the labs; am I correct?

Mr. PODONSKY. Yes, sir.

Mr. BURR. So clearly everybody knew there was a lack of understanding, or there wouldn't have been a need for a memo; safe to say?

Mr. PODONSKY. Yes.

Mr. BURR. Since this was a DOD project, was DOD involved in the security requirements for the NEST program?

Mr. PODONSKY. I am not conversant on that. I would defer that to General Boomer—or I would say General McBroom.

Mr. BURR. Let me just say, Mr. Chairman, that it is my understanding from staff that the committee did make an invitation of DOD to participate in this hearing. They did not accept our invitation. I am sorry that they didn't because I would hope that anybody who had relevant information would be willing to come in.

One last question, if I could, from the standpoint of the individual in charge of independent oversight and the extensive work that you have done in the labs, do you have any recommendations to this subcommittee and to the three directors of those labs that are in our audience and here testifying after you, about the dual use of vaults in the future and if you have any specific comments about the dual use of the vault that NEST equipment kits were kept in?

Mr. PODONSKY. I would say that, Congressman, we addressed that with our recommendations for a closer look at the need-to-know policy, but for a general statement I would say, as—I would like to iterate the point I said earlier, is that the fingerpointing

needs to cease between the lab and the Department, as well as the legislative arm and the executive branch, and we need to get on with fixing our national security interests.

Mr. BURR. I agree with you totally. I hope I am—I hope I understand correctly what took place in that vault facility. I think even a layman would agree that if you have got two separate projects in there, and you have got individuals who are approved for one and not approved for the other and vice versa, all with the ability to go in alone, that you have got a potential breach. It doesn't mean that one will happen, but you have got the opportunity for a breach of that information to happen.

As a security expert, would you agree with that?

Mr. PODONSKY. Yes, sir.

Mr. BURR. So it is probably a policy that we ought to look at very seriously in the future about the dual use of a secure facility?

Mr. PODONSKY. Yes, sir.

Mr. BURR. Okay. I thank all of our witnesses, and I yield back.

Mr. UPTON. Thank you. Mr. Cox.

Mr. COX. Thank you. Before I leave the subject of polygraphs, I note that in the Interim Report to the Secretary of Energy on the Control of Classified Weapons Data at the National Weapons Laboratories—which I believe, Mr. Podonsky, you have provided?

Mr. PODONSKY. Yes, sir.

[The information referred to follows:]

REDACTED VERSION

Interim Report

Special Review

Interim Report
to the
Secretary of Energy

on the

Control of Classified Weapons Data
at the National Weapons Laboratories

Office of
Independent
Oversight and
Performance
Assurance

June 2000

REDACTED VERSION

PREFACE

This is an interim report to the Secretary of Energy of the special review by the Office of Independent Oversight and Performance Assurance (OA). It is only an interim report because the special review has not been completed. OA will not be able to access the Los Alamos National Laboratory facility until the FBI has completed its investigation. At the conclusion of the FBI investigation, OA will resume its special review for the Secretary and a final report will be issued.

REDACTED VERSION

SPECIAL REVIEW

A REPORT TO THE SECRETARY OF ENERGY ON THE CONTROL OF CLASSIFIED WEAPONS DATA AT THE NATIONAL WEAPONS LABORATORIES (U)

Table of Contents (U)

Executive Summary 4

1.0 Introduction 8

2.0 Background 9

3.0 Security Program Effectiveness 13

4.0 Conclusions and Recommendations 21

APPENDIX A Supplemental Information 24

APPENDIX B Sandia National Laboratories-New Mexico 25

APPENDIX C Lawrence Livermore National Laboratory 33

This page contains Unclassified information.

REDACTED VERSION

REDACTED VERSION

ACRONYMS (U)

ACRONYM	DEFINITION
AL	Albuquerque Operations Office
ARG	Accident Response Group
CAS	Classified Administrative Specialist
CD	Compact Disc
CDPO	Classified Document Project Office
CFR	Code of Federal Regulations
CMPC	Classified Matter Protection and Control
DNS	Director of Nuclear Security
DNT	Defense Nuclear Technology Directorate
DoD	Department of Defense
DOE	Department of Energy
DP	Office of Defense Programs
FBI	Federal Bureau of Investigation
GSA	General Services Administration
ICF	Inertial Confinement Fusion
JTOT	Joint Technical Operations Team
LADS	Livermore Administrative Document System
LAMPIS	Laboratory Management Program for Integrated Security
LAN	Local Area Network
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
NEST	Nuclear Emergency Search Team
NNSA	National Nuclear Security Administration
NNSI	Nonproliferation and National Security Institute
NWIB	Nuclear Weapons Information Base
OA	Office of Independent Oversight and Performance Assurance
OAK	Oakland Operations Office
OPSEC	Operations Security
PAP	Personnel Assurance Program
PSAP	Personnel Security Assurance Program
S&S/ES&H	Safeguards and Security/Environment, Safety and Health
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SNL	Sandia National Laboratory
SNL-NM	Sandia National Laboratory-New Mexico
SO	Office of Security and Emergency Operations
SUCI	Sensitive Use Control Information
TSCM	Technical Surveillance Countermeasures
U.S.	United States

Information on this page is Unclassified

REDACTED VERSION

REDACTED VERSION

EXECUTIVE SUMMARY (U)

(U) In response to a security incident at the Los Alamos National Laboratory (LANL) involving missing classified hard drives, the Secretary of Energy, Bill Richardson, directed the DOE Office of Independent Oversight and Performance Assurance (Independent Oversight) to examine the adequacy of controls at Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratories-New Mexico (SNL-NM). The Secretary initially directed the Independent Oversight team to perform a review at LANL. Subsequently, in accordance with discussions among Independent Oversight, the Federal Bureau of Investigation (FBI), and the U.S. Attorney, it was determined that the FBI investigation covers areas that overlap the planned Independent Oversight review. Therefore, in consultations with the Secretary, it was decided to delay the LANL review until the FBI investigation is completed. A similar review of LANL will be conducted when the ongoing FBI investigation is complete.

(U) The purpose of the review was to provide an expedited assessment of the adequacy of protection measures in place for selected high-priority classified information. In addition to examining the sites' protection effectiveness, the Independent Oversight team also reviewed the adequacy of DOE policy as it related to protection of classified weapons data.

(U) Over the past ten years, many of the requirements that previously mandated DOE sites to establish formal accountability systems for classified information were eliminated. The decisions to eliminate accountability requirements had their foundation in a 1990 National Security Council assessment and were based on Executive Orders, which eliminated national requirements for formal accountability for classified documents. The reduction in the requirements for accountability is one part of the general trend toward a reduction in security that occurred in the early to mid 1990s. In that period, DOE was focusing on reducing security costs, declassification, and increasing "openness" of DOE sites to promote interactions with the community and industry. DOE Headquarters prompted sites to reduce costs through downsizing protective forces, downgrading clearances, and eliminating or consolidating security areas.

(U) In 1999, the reported security violations at LANL involving downloading of classified nuclear weapons data focused attention on protection of nuclear weapons design information at the national laboratories. Extensive and unprecedented Secretarial-level attention was placed on security within DOE with special emphasis on the three weapons laboratories. Secretary Richardson directed numerous actions to address security problems at the national weapons laboratories, such as directing implementation of an extensive set of cyber security enhancements. Concurrently, Secretary Richardson took actions to enhance DOE's management of security, including reorganizing the security functions, elevating oversight, adding experienced personnel to provide direction to the security program, adding expertise in counterintelligence, implementing a polygraph program, issuing a zero tolerance policy, and other such measures. Under the leadership of the Secretary, the laboratories took many aggressive actions such as intensifying security awareness, establishing a strong disciplinary action program, increasing control of foreign nationals, enhancing cyber security firewalls, enhancing classified parts storage, and increasing the resources and management support for security programs.

(U) This review determined that, in general, LLNL and SNL-NM comply with the minimum DOE requirements for administrative control of classified matter in the areas reviewed by the Independent Oversight team. Specifically, the laboratories are properly implementing the DOE requirements for storing documents, including lock combination changes as required by DOE policy, destroying documents (e.g., use

REDACTED VERSION

of approved destruction methods, required recordkeeping), and controlling access to vaults and vault-type rooms containing classified weapons data.

(U) Both laboratories are implementing proactive programs for providing enhanced security for especially sensitive assets, such as those maintained for offsite emergency response teams (e.g., the Nuclear Emergency Search Team - NEST). For example, SNL-NM maintains full accountability for Top Secret information. These systems, used to account for Top Secret and Sigma 14 documents, were complete and accurate (based on a sample examined by Independent Oversight). Overall, although ongoing initiatives and resolution of some pending issues remain to be completed, SNL-NM is effectively implementing protection requirements for classified weapons data and is currently guiding its protection program on an upward, improving course.

(U) LLNL has implemented a program for classified matter protection and control that largely complies with DOE orders. Procedures are current and observations during this review indicated that document marking, document transmittal, document transfer, and document destruction are performed in conformance with DOE requirements and local procedures. Separate reviews of the LLNL Top Secret accounts and the LLNL Sigma 14 and 15 account revealed that all accountable documents were appropriately controlled and properly safeguarded. The limited access to Sigma 14 data allowed by the LLNL Use Control Facility Coordinator is an especially effective practice. While additional management attention is warranted in a few areas, LLNL is adequately implementing requirements for the protection and control of classified weapons data.

(U) However, as a result of the Government-wide reduction in security requirements noted above, LLNL and SNL-NM, like LANL and other DOE and government sites no longer have systems that can assure detection of a loss of classified matter or determine who has custody of classified matter at a given time. The current national requirements for controlling classified matter are not as stringent and clear as needed in light of DOE's particularly sensitive nuclear-weapons-related information; improvements in policy are needed to further enhance security at DOE sites.

(U) At the laboratories, as at all DOE sites, there are two threats to classified information to be considered: the outsider threat – people with no authorized access to the information - and the insider threat – people who need to access information as part of their job. Protection against the outsider threat is provided by physical security – guns, gates, guards, locks, and alarms – and administrative controls, such as procedures to check the identity of personnel entering vaults to ensure that they are authorized and have a need to know.

(U) Protection against the insider is the most challenging part of security. Certain personnel need access to the information to do the job they are paid to do – such as serve on NEST teams to respond to a nuclear emergency. Although many measures are in place to protect against an insider, such as personnel security programs and security awareness, it is important to recognize that these controls do not eliminate the insider threat or the potential for compromise of information through errors or violations of procedures.

(U) Secretary Richardson has again taken prompt and aggressive actions to address residual weaknesses that have become apparent in the course of security incidents. On June 19, 2000, the Secretary issued directions to enhance classified matter protection. For example, he specifically required nuclear weapons laboratories to immediately implement measures to better control entry and egress to vaults, including mandating that logs be kept. The Secretary also directed a near-term comprehensive evaluation of existing vault procedures, encryption of certain stored data, accountability for certain media, an inventory of certain electronic media, and other measures

to enhance security on an expedited basis. On June 23, 2000, the DOE Office of Defense Nuclear Security within the National Nuclear Security Administration developed implementing guidance for the Secretary's direction. LLNL and SNL-NM have taken some immediate actions to implement this direction and are aggressively working to address all the directed actions.

(U) The Secretary's enhanced protection measures and the recent implementing guidance provide a good framework for improving protection on an immediate and near-term basis. While the review at LANL has not been completed, the following interim additional actions are recommended to complement the recent direction and implementing guidance on a longer-term basis.

REDACTED VERSION

RECOMMENDATIONS

Re-institute requirements for a formal accountability system for certain types of information.

- Top Secret and Secret Restricted Data related to nuclear weapons should be included.
- An evaluation is needed to determine whether other Secret Restricted Data related to production of special nuclear materials and nuclear energy should be included.
- Commercially available technologies (database, bar codes, etc.) should be used to facilitate implementation.

Establish a clear and comprehensive graded approach and issue appropriate implementing guidance.

- Needs to incorporate additional measures for accounting for and tracking more sensitive types of documents.
- The recent enhancements for vaults need to be expanded to include other types of storage repositories.
- It should include practical guidelines for categorizing the relative importance of security interests.

Clarify the need-to-know policy.

- Expectations for partitioning information within large storage areas.
- Prudent measures to restrict access to those with a specific need to know.

Continue efforts to expand the human reliability programs.

- Participation in human reliability programs should be considered as a control in a graded approach to protection.
- The parameters of DOE programs should be reevaluated to ensure that they are designed to provide assurance of an individual" trustworthiness (e.g., polygraph examinations).

Conduct a review of special access programs and sensitive compartmented information.

- These programs should be reviewed in a manner similar to this effort.

Develop a plan and milestones for revising and reissuing the DOE orders and manuals to reflect recent and planned policy changes.

- The changes directed by Secretary Richardson need to be refined and then incorporated into DOE directives on an expedited basis
- Other changes recommended above should also be made as soon as possible.
- In particular, SO should accelerate efforts to develop and issue guidance to SNL regarding the protection of classified parts.

REDACTED VERSION

SPECIAL REVIEW

A REPORT TO THE SECRETARY OF ENERGY ON THE CONTROL OF CLASSIFIED WEAPONS DATA AT THE NATIONAL WEAPONS LABORATORIES (U)

I Introduction (U)

(U) In June 2000, the Secretary of Energy was informed of a security incident at the Los Alamos National Laboratory (LANL) involving missing hard drives. These hard drives contained highly sensitive classified information about nuclear weapons designs and methods of disabling nuclear weapons and devices. The hard drives were found to be missing from a vault used to store classified documents and electronic storage media (e.g., disks, hard drives, etc.). With the full support of DOE, the Federal Bureau of Investigation (FBI) is conducting an investigation of the incident.

(U) Because of the potentially serious nature of the LANL security incident, the Secretary also took aggressive steps, such as requiring logging of access to vaults and requiring accountability for particularly sensitive assets, as documented in a June 19, 2000 memorandum entitled *Enhanced Protection Measures*. As one of the Secretarial actions, the Secretary directed the DOE Office of Independent Oversight and Performance Assurance (Independent Oversight) to examine the adequacy of security procedures and administrative controls at the three nuclear weapons laboratories. The purpose of the review was to provide an immediate assessment of the adequacy of measures in place for some of the highest-priority classified information. The team also looked at the enhanced controls directed by the Secretary in the June 19 memorandum to determine whether the sites had taken actions for the measures that were to be "effective immediately" and whether they were developing plans to implement the other provisions.

(U) The first portion of the review was conducted during the period from June 17 through June 23, 2000, and is documented in this report. For this portion of the review, the Independent Oversight team reviewed the control of highly-sensitive classified matter as implemented by selected organizations at Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratories – New Mexico (SNL-NM). At LLNL, the team focused on the Defense and Nuclear Technologies Directorate. At SNL-NM, the team focused on the Weapons Systems organization and the Defense Programs Products and Services organization.

(U) The Secretary also initially directed the Independent Oversight team to perform a review at LANL. Subsequently, in accordance with discussions among Independent Oversight, the FBI, and the U.S. Attorney, it was determined that the FBI investigation covers areas that overlap the planned Independent Oversight review. Therefore, in consultations with the Secretary, it was decided to delay the LANL review until the FBI investigation is completed.

(U) For each of the organizations reviewed, the Independent Oversight team focused on the controls of most sensitive classified assets, such as:

- (U) Information about disabling nuclear weapons, including U.S., foreign and postulated improvised designs that a

REDACTED VERSION

terrorist might use. Such information is similar to that provided to the Nuclear Emergency Search Team (NEST) and contained on the LANL hard drives noted above.

- (U) Top Secret information, which is defined as information that, if compromised, could cause grave damage to the United States.
- (U) Secret Restricted Data regarding the design of U.S. nuclear weapons.
- (U) Sensitive Use Control Information (SUCI) which is a subcategory (Sigma 14 and 15) of Secret Restricted Data that encompasses methods for enabling a nuclear weapon to detonate.

(U) Within this limited scope, Independent Oversight selectively examined key aspects of no protection, including generation, storage, marking, destruction, and control of access to the information. The team focused on access controls at vaults and other storage areas, accountability/tracking systems where implemented, storage mechanisms, and implementation of the "need to know" requirements. The review team also focused on the role of site management in ensuring that DOE policies related to control of classified matter are established and implemented within the selected organizations. To assess management effectiveness, Independent Oversight assessed four general principles of security management: line management responsibility for security, personnel competence and training, comprehensive requirements, and feedback and improvement. Data for this review was collected through a variety of methods, including document reviews, observations, interviews, and limited scope performance testing.

(U) In addition to examining the site's compliance with current policy, the Independent Oversight team also reviewed the adequacy of current policy as it related to protection of classified matter. In many cases in the past, Independent Oversight had determined that sites were complying with the established requirements but that the security interests were not provided sufficient protection because the applicable DOE policies are not sufficiently clear or comprehensive (e.g., graded approach). In such instances, Independent Oversight developed policy issues or transmitted its concerns to the DOE organization responsible for security – the Office of Security and Emergency Operations (SO).

(U) This initial limited scope Independent Oversight special review was completed in a short time to provide timely feedback to the Secretary. In addition to the plans for review at LANL when the FBI investigation is complete, Independent Oversight will conduct follow-up activities as appropriate. Further, Independent Oversight has previously scheduled activities during the summer/autumn of 2000 at all three nuclear weapons laboratories to review selected security programs, interim measures, and progress on corrective actions for previously identified deficiencies.

(U) Section 2 of this report provides background information about DOE policies related to protection of classified matter, including a brief chronology of the elimination of accountability requirements. Section 3 provides the results of the review, including summary assessments of LLNL and SNL-NM as well as a review of policy. Section 4 provides the overall conclusions and recommendations. Appendix A identifies the composition of the Independent Oversight team for this phase of the review. Appendices B and C present more detailed discussions of the observations of the effectiveness of the SNL-NM and LLNL programs, respectively.

2 Background (U)

(U) The requirements for protection of classified matter are delineated in DOE Order 471.2A, Information Security Program, and the associated DOE Manual 471.2-1B, and other applicable DOE orders and manuals. These

documents establish specific requirements for access authorization/control, accountability, storage, transmittal/receipt, classification and marking, reproduction, and destruction. These requirements encompass classified documents and other forms of classified matter, such as nuclear weapons parts and electronic storage media.

(U) Although the scope of this review focuses on administrative controls for protection of classified matter, it is important to recognize that requirements for protection of classified matter are one element of a multi-faceted security program that also includes physical security (e.g., intrusion alarm systems), protective forces, and personnel security. In addition, DOE has a classified computer security program for protecting classified information on computer systems and networks.

(U) At the fundamental level, there are two threats to classified information that are considered: the outsider threat – people with no authorized access to the information and the insider threat – people who are granted access to information as part of their job. Protection against the outsider threat is provided by physical security – guns, gates, guards, locks, and alarms – and administrative controls, such as procedures to check the identity of personnel entering vaults to ensure that they are authorized and have a need to know. Protection against the insider is the most challenging part of security. Certain personnel need access to the information to do the job they are paid to do – such as serve on NEST to respond to a nuclear emergency. There are many measures in place to protect against an insider: personnel security programs, security awareness, human reliability programs, polygraphs for certain categories of employees, "need to know" controls, counterintelligence programs, and, most importantly, accountability for protection.

(U) Although a security clearance is a prerequisite, people must have a "need to know" before being given access to classified information. A need to know is based on a management decision that the individual needs particular types of information to perform their official duties. The application of the need to know principle is intended to narrow the window of vulnerability to the insider threat by limiting the number of personnel with access to information to as few as possible, consistent with mission needs.

(U) Key components of a classified matter protection program include:

(U) **Identification and Markings** Classified matter must be appropriately identified and clearly marked with the classification level (Confidential, Secret, and Top Secret) and category (Restricted Data, Formerly Restricted Data, and National Security Information).

(U) **Controls on Transmittal**. Classified matter may only be transmitted in the performance of official duties and in accordance with approved methods, which depend on the classification level and category. For example, Secret and Confidential may be transmitted via the U.S. Postal Service while Top Secret may not – Top Secret must be transmitted by the Defense Courier Service or Department of State Courier System.

(U) **Secure Storage**. The matter must be in approved containers and locations. Typically, classified matter is stored in an approved security container (e.g., a vault or a GSA-approved safe) which is further protected by some combination of alarms or protective force patrols.

(U) **Personnel Security**. A formal personnel security program is in place to determine whether individuals are eligible for access to classified information at the various levels and categories.

(U) **Access Controls**. Access is restricted to personnel with a clearance and a need to know. Custodians of information are responsible for controlling access to classified information. Access is normally enforced through physical methods (e.g., combination

locks) and administrative controls (e.g., access lists of approved individuals).

(U) **Human reliability program**. The DOE human reliability programs (i.e., the Personnel Security Assurance Program or the Personnel Assurance Program) are additional personnel security measures currently used primarily for personnel with access to special nuclear material or nuclear explosives. The human reliability programs add additional measures such as random drug testing and psychological screening. They also include supervisory training on the identification of aberrant behavior.

(U) DOE policy recognizes that certain information is more sensitive than other information. For example, the requirements for storage of Top Secret documents are marginally more stringent than for Confidential documents. In addition, DOE policy requires a "graded approach" for protection of classified matter. This graded approach is intended to ensure that the protection is commensurate with the importance of the security interest. For example, the Manual indicates that "information which would assist an adversary in the development of a nuclear weapon, or information that would assist an adversary in bypassing use control systems, could have consequences so grave as to demand the highest attainable standard of security."

(U) The LANL hard drive incident prompted many questions about the lack of a system for accounting for the hard drives and related practices, such as logging access to areas where classified matter is stored. As discussed in the following paragraphs, over the past ten years, DOE has eliminated many of the requirements that previously compelled DOE sites to maintain a formal accountability system.

(U) Prior to 1991, DOE required a formal accountability system for all Secret and Top Secret classified matter (Confidential information had never been subject to formal accountability). The formal accountability required that:

- (U) An accountability system for all Top Secret and Secret matter that used a special numbering system, such that each document/item had a unique number
- (U) The accountability system covered documents/items from origination through destruction or transfer to another site
- (U) Special markings, page numbering, copy number, and series designation on every document
- (U) Establishment of a chain of custody such that each document/item was assigned to an individual who was responsible for its protection (this typically entailed receipt and transfer forms and sign out sheets for each document)
- (U) The conduct of periodic inventories to ensure that documents were present and accounted for and that the accountability records were complete and accurate.

(U) In February 1991, DOE modified its policy such that sites were no longer required to account for some types of Secret matter. Specifically, DOE no longer required accountability for Secret matter that was categorized as National Security Information or non-weapons Restricted Data (i.e., related to production of special nuclear materials or energy). The relaxation of the accountability requirements had its foundation in a National Security Council assessment in 1990, which was intended to establish an efficient single industrial security program for industry and government.

(U) In May 1992, DOE again modified the requirements based on the provisions of 32 CFR XX. This change eliminated the requirement to maintain formal accountability for Secret Restricted Data that involved nuclear weapons information.

(U) In January 1998, DOE also eliminated the requirements for formal accountability for Top Secret information. This decision was made under the authority of Executive Order 12958, which was issued in April 1995 and which eliminated national requirements for formal accountability for Top Secret matter.

(U) With these modifications, DOE sites are only required to maintain accountability systems for certain types of documents, such as foreign government and SUCI information. Certain special access programs, sensitive compartmented information, and work for others programs may also require formal accountability systems. The total number of documents/items currently required to be placed in a formal accountability system is a very small fraction of the total classified inventory.

(U) With the elimination of the formal accountability system requirement, DOE sites no longer were required to maintain unique document numbers, keep accountability records of documents, perform routine inventories, annotate copy and series, certify destruction, or require written authorization to reproduce a Secret document. Sites were still required to meet other requirements such as those related to storage, access controls, and marking.

(U) The reduction in the requirements for accountability is one part of a general trend toward a reduction in security that occurred in the early to mid 1990s, partly as a result of the end of the cold war. In that period, DOE was focusing on reducing security costs, declassification, and increasing "openness" of DOE sites to promote interactions with the community and industry. DOE Headquarters prompted sites to reduce costs through downsizing the protective forces, downgrading clearances, and eliminating or consolidating security areas. While some of these efforts did result in equivalent security and reduced costs, some decisions were made without careful planning and analysis of security needs, resulting in a degradation of security effectiveness at some sites and laboratories.

(U) In 1997, senior DOE management recognized that degradations in security needed to be addressed. As one action, the predecessor organization of the Office of Independent Oversight and Performance Assurance conducted a review of all major DOE sites to develop a profile of the sites and the problems. As a result of this review and senior management attention, significant efforts to enhance security were initiated, with most of the initial emphasis being placed on protection of special nuclear material. As the special nuclear material weaknesses were addressed, Independent Oversight began to increasingly focus on protection of classified and sensitive information, with particular emphasis on classified parts and cyber security.

(U) In 1999, the allegations of espionage at LANL and the reported associated security violations involving downloading of classified nuclear weapons data focused attention on protection of nuclear weapons design information at the national laboratories. Extensive and unprecedented Secretarial-level attention was placed on security within DOE with special emphasis on the three weapons laboratories, and Independent Oversight conducted inspections and follow-up reviews at all three national weapons laboratories. Secretary Richardson directed numerous actions to address security problems at the national weapons laboratories, such as implementation of an extensive set of cyber security enhancements (i.e., the nine-point plan and the six further enhancements). Concurrently, Secretary Richardson took actions to enhance DOE's management of security, including reorganizing the security functions, elevating oversight, adding experienced personnel to provide direction to the security program, adding expertise in counterintelligence, implementing a polygraph program, issuing a zero tolerance policy, and other such measures. In the same time frame, the DOE Headquarters Office of Defense Programs (DP) issued the goal post memorandum, which defined DOE expectations for near term improvements to achieve a satisfactory program. Under the leadership of the Secretary, the laboratories

took many aggressive actions such as intensifying security awareness, establishing a strong disciplinary action program, increasing control of foreign nationals, enhancing cyber security firewalls, enhancing classified parts storage, and increasing the resources and management support for security programs. The recent Independent Oversight reviews concluded that the laboratories had addressed identified weaknesses (including longstanding weaknesses with classified parts), met DOE expectations defined in the goal post memorandum, and generally met current DOE requirements.

Security Program Effectiveness (U)

(U) The results are presented in three subsections. The first two provide a summary of observations regarding, implementation of policy at LLNL and SNL-NM; more detailed information is included in appendices to this report. The third subsection discusses the adequacy of policy.

3.1 Sandia National Laboratories – New Mexico (U)

(U) Overall, SNL-NM is adequately implementing requirements for the protection and control of classified matter. In some instances, SNL has instituted additional protection measures that are not specifically required by the DOE Order or Manual. For example, the laboratory has retained full accountability for Top Secret matter, which is not specifically required. In addition, the site has recently enhanced their control of certain computer media maintained for emergency response to include accountability, frequent inventories, and two-person control.

(U) There is ample evidence that a major programmatic reorganization aimed at placing responsibility for security in the hands of line managers is gaining acceptance and taking hold in line organizations. This and other initiatives reflect significant senior laboratory management support for safeguards and security. Examples of positive aspects of the program and recent enhancements include:

(U) SNL has implemented standardized procedures and other guidance for controlling classified matter, and has made them easily available to all employees by placing them on-line on the laboratory's internal network.

(U) Systems used to account for Top Secret and Sigma 14 documents were complete and accurate (based on a sample examined by Independent Oversight).

(U) The laboratory has made a significant effort to store all classified parts in approved security configurations. Lock combinations are changed as required by DOE Orders. Where needed, adequate compensatory measures remain in place at classified material storage locations, pending guidance from SO.

(U) Personnel responsible for controlling classified documents demonstrated clear understanding of their responsibilities and the required procedures, and had the necessary resources available.

[REDACTED PARAGRAPH]

(U) Additional management attention is also needed in certain aspects of the management systems that support the classified matter protection program. SNL-NM is not currently implementing a comprehensive self-assessment program. Also, certain administrative aspects of the training program for classified document custodians need to be improved, and program guidance needs to be updated. In these areas, SNL has ongoing or planned efforts to make the needed enhancements. In addition, more consistency and rigor in the approach to determining need to know is warranted in some SNL-NM divisions.

(U) Overall, although ongoing initiatives and resolution of some pending issues remain to be completed, SNL-NM is effectively implementing protection requirements for classified weapons data and is currently guiding its protection program on an upward, improving course.

3.2 Lawrence Livermore National Laboratory (U)

(U) LLNL has implemented a CMPC program that largely complies with DOE orders. Procedures are current and observations during this review indicated that document marking, document transmittal, document transfer, and document destruction are performed in conformance with DOE requirements and local procedures. Lock combinations are changed as required by DOE Orders. Written desktop procedures were available to assist personnel in addressing both site-wide and organizational requirements. Separate reviews of the LLNL Top Secret accounts and the LLNL Sigma 14 and 15 account revealed that all accountable documents were appropriately controlled and properly safeguarded. The limited access to Sigma 14 data allowed by the LLNL Use Control Facility Coordinator is an especially effective practice. Further, LLNL maintains an administrative document system to track access to selected documents that can be used to identify a document, control access to it, and determine who has authorized access to it.

(U) The CMPC training program is comprehensive and effective, and there are adequate training assets to prepare future employees for CMPC duties. Performance tests performed during this review indicate that personnel and managers with responsibilities for CMPC are knowledgeable of their duties and are capable of performing them. Their position descriptions include their CMPC responsibilities, and their performance ratings include their effectiveness in performing CMPC-related duties.

(U) The newly revised CMPC self-assessment program represents a new approach with promise for enhancing self-assessments and providing meaningful management feedback concerning the CMPC program. There is evidence that the results of self-assessments, DOE surveys, and other audits are addressed at appropriate management levels and effective action taken.

(U) Further, LLNL management has supported a proactive program of identifying especially sensitive information assets and providing enhanced protection for them. Prior to this review, LLNL management had undertaken to address the need to enhance protection for some critical and sensitive assets and had also begun a comprehensive review of LLNL vaults and vault-type rooms to determine potential protection weaknesses. The results of this review are scheduled to be available within one week, and LLNL managers interviewed indicated strong support for implementing the expected results of that review.

[REDACTED PARAGRAPH]

[REDACTED PARAGRAPH]

[REDACTED PARAGRAPH CONTINUED]

(U) As evidenced by the results of this review, LLNL has demonstrated strong management involvement in efforts to protect classified weapons data in its custody. While additional management attention is warranted in a few areas, LLNL is adequately implementing requirements for the protection and control of classified weapons data.

3.3. DOE Policy (U)

(U) As discussed in Section 2, DOE has a multi-faceted policy in place for protecting classified matter, including the most sensitive types of classified matter that were the focus of this review. The general principles (restricting access, ensuring trustworthy individuals, and need to know) are sound and are consistent with other U.S. government agencies. However, notwithstanding the aggressive instructions issued on June 21, 2000, the results of this review, in combination with the results of previous Independent Oversight inspections and reviews, indicate that there are weaknesses in policy that require significant and timely management attention. These weaknesses are discussed under the five general categories of: relaxation of accountability requirements, lack of specificity in DOE requirements, lack of direction regarding implementation of the need to know principle, over reliance on individual compliance, and inadequate definition of the graded approach.

Changes in Accountability Requirements (U)

(U) The relaxation of changes in the accountability requirements has resulted in some increase in operational efficiency and reduced costs. For example, laboratory personnel save time and effort because they no longer need to track each document (e.g., receipts) and are not required to perform certain administrative functions (e.g., obtaining permission to make copies and marking each copy). Similarly, DOE sites no longer have to expend resources conducting periodic inventories, which could encompass millions of documents at nuclear weapons laboratories.

(U) The increased operational convenience and reduced costs, however, came with a corresponding reduction in certain aspects of security. In the absence of a formal accountability system, DOE sites no longer have the capability to determine important information such as whether a document/item is missing, where specific documents are located, who has had access to those documents, who has responsibility for control and protection, and whether a document has been destroyed. In addition, DOE sites generally cannot track documents/items to determine who has responsibility for them in the event one is determined to be missing. DOE sites are also limited in their ability to ensure that individuals are held accountable for implementing security requirements because there is usually no way to determine who has direct responsibility for a missing document or who last had access to the document.

(U) After the LANL hard drive incident, DOE and LANL were severely criticized for LANL's lack of capability to detect a loss, determine who has been in a vault and when, or determine who has custody of a document/item at a given time. LANL did not have this capability even for hard drives that contained information that was among the most sensitive in the complex. Also, the LANL loss was discovered as a result of an unscheduled check because of a fire rather than as part of a systemic inventory. However, the situation at LANL is not unique to the LANL X Division vault. In fact, the same situation is evident at LLNL and SNL-NM and essentially every other DOE site as well as other government agencies. Within LLNL, for example, there are about a million classified documents, about five thousand of which are in a formal accountability system. Without systems in place to track and account for documents, the

protection system's ability to detect a loss or find the person who should have custody is limited.

(U) It is important to recognize that re-establishment of an accountability system does not eliminate the insider threat or the potential for compromise of information through errors or violations of procedures. Even with an accountability system in place, an insider (i.e., an authorized person intent on espionage) could still make unauthorized copies of documents or electronic media. However, strengthened systems for accountability and tracking, in combination with other measures (e.g., controlling access to copiers and data transfer devices), would strengthen individual accountability and improve security by increasing the deterrence factor and the likelihood of detecting an unauthorized act.

(U) DOE followed the Executive Orders and practices of other government agencies in deciding to relax accountability requirements. In some ways, DOE has comparable security concerns to other agencies and a common approach is warranted. For example, DOE sites have national security information that is similar to that possessed by other agencies. However, DOE sites and laboratories have unique concerns that other agencies do not face, most notably design information related to nuclear weapons and extremely sensitive information about use control and disablement of nuclear weapons. The DOE Headquarters Office of Defense Programs and SO have made some efforts to convince the Department of Defense (DoD) that some changes were needed to better protect sensitive classified matter (e.g., reevaluating classification and protection of certain types of information). However, those efforts have not been embraced by DoD.

(U) The DOE decisions to eliminate formal accountability for Secret and Top Secret matter were controversial at the time and continue to be so. Some organizations, including the predecessor to Independent Oversight, commented on the inevitable degradation in rigor and formality of handling classified matter following the 1991 and 1992 decisions to relax accountability requirements. Similarly, the 1998 decision to eliminate formal accountability for Top Secret matter did not receive universal support. Although not mandated, all three national laboratories have retained some aspects of their accountability systems for Top Secret and SNL-NM has maintained a full formal accountability system.

(U) Various DOE elements and individuals have advocated re-establishment of a formal accountability system for Top Secret documents and/or Secret weapons data. Most notably, in March 1999, the Directors of the three nuclear weapons laboratories sent a joint recommendation to the DOE Under Secretary and the DOE Director of the Office of Counterintelligence in which they advocated that DOE reinstate accountability for documents that contain Secret Restricted Data and Top Secret Restricted Data. They indicated that, without formal accountability, counterintelligence reviews are much more difficult because it is not feasible to determine specifically who has had access to certain design information. They also cite the Cox Commission report as a basis for reinstating formal accountability.

(U) Although re-establishment of a requirement for an accountability system is an important step, additional actions will be needed to ensure that the accountability systems are effective. The current requirements for accountability are not sufficiently detailed to provide adequate direction to the field to ensure a complete chain of custody. In addition, accountability systems need to be viewed as one element of a viable and comprehensive graded approach to protection (as discussed later in this section, DOE has a graded approach concept but the current guidance is not adequate).

(U) As part of the June 21, 2000 Office of Defense Nuclear Security within the National Nuclear Security Administration (NNSA/DNS) implementing guidance for Secretary of Energy June 19, 2000 memorandum, direction has been provided to DOE field elements to place certain

materials (i.e., computer media that have a compilation of nuclear weapons design and testing information that contains Sigma 1, 2, 14, or 15 information) into an accountability system. Specific methods for implementing the accountability system are included in the guidance.

Lack of Consistency and Specificity in DOE Requirements (U)

(U) As discussed in Section 3.1 and 3.2 and Appendices B and C, SNL-NM and LLNL generally comply with the minimum requirements specified in the DOE Order and Manual, although each site has some specific weaknesses that need to be addressed. However, the protection effectiveness for similar information varies considerably from place to place and does not provide a level of protection that is based on the sensitivity of the information.

(U) For example, at SNL-NM, some Secret Restricted Data documents containing weapons design information were stored in a GSA-approved container within a vault-type room where it is provided alarm protection with a protective force response time of 15 minutes or less. DOE policy would permit a copy of the same document to be stored in a GSA-approved security container equipped with a specified lock within the Sandia limited area (anywhere within the fenced area). In one case, a penetration of the vault-type room repository would be responded to within 15 minutes; in the other case, no alarm would sound and a penetration of the repository would not be noted until someone happened to inspect the container and notice a breach (there are no specific requirements for protective force patrols at any interval in this case). Both of these situations, however, comply with the requirements for storage of Secret matter as specified in DOE Manual 471.2-1B.

(U) As part of a DOE-wide effort to revise DOE orders to allow the field more flexibility in determining how to implement general requirements, the Information Security Program Order (DOE 471.2A) was revised in 1997. As part of the increased flexibility, the current Order contains only very general and vague requirements (e.g., "controls shall be established to detect and deter unauthorized access to classified matter"). For some aspects of protection, the associated Manual provides more detailed requirements. However, the Manual does not provide much information on important subjects such as access controls at vaults. In the absence of specific requirements, DOE sites, which are under continued pressure to reduce costs and/or justify expenditures based on DOE order requirements, often decide to implement only the minimum requirements as specified in the Order or Manual.

(U) The results of this review and recent inspections indicate that the lack of specificity and clarity in policy is a contributor to inconsistent protection effectiveness. Supporting examples include:

(U) **The DOE Order and Manual require access controls but provide no specific information on requirements for access to vaults and vault-type rooms.** For example, there is no information on requirements for logs of entry and exit times. The approaches varied considerably between the national laboratories and between different areas in the same laboratory. As noted in the LANL incident, no logs were kept at the X Division vault at LANL for personnel on the access list. At SNL-NM, card reader systems were used at some areas such that there was a log of the entry but these systems were not implemented in a way that provided a comprehensive log (e.g., there were no mechanisms or procedures to prevent "piggy backing" in which additional personnel enter after one person opens the door) and there were no mechanisms to log when an authorized person exits. The Secretary's June 19, 2000 enhancements specifically require immediately implementing measures to record the time of entry and egress. The Secretary also directed a near-term comprehensive evaluation of existing vault procedures, revision of policies, and rapid implementation. LLNL and SNL-NM have taken some immediate actions to implement this

direction and are aggressively working to address all the directed actions.

(U) **Requirements for locks are not comprehensive.** DOE requirements have provisions for changing repository lock combinations in certain conditions (e.g., when personnel with the combination are terminated). Previous versions of the orders included provisions for changing the locks on an annual basis; these requirements were dropped in the latest revision. The sites are not required to, and generally do not, have a program in place to change the lock combinations on a regular basis. The absence of a specific requirement creates the potential for a lock combination to go unchanged for many years, potentially compounding the damage associated with a compromised combination. In addition, DOE sites, including LLNL and SNL-NM, often use temporary measures (day locks or keypad locks instead of combination locks) for short time periods (e.g., up to an hour while the individual is on a break). There are few provisions in the Orders or Manuals that discuss how and when such alternative methods provide acceptable security. The recent Secretarial direction and NNSA/DNS implementing guidance place restrictions on this practice in vaults.

(U) **DOE policies make no real distinction between documents and electronic media with respect to storage and control.** Most of the requirements in DOE orders were written before the advances in cyber technology and were primarily developed with paper documents in mind. For the purposes of protection of classified matter, an electronic media item (e.g., a hard drive or compact disk) is treated the same as a document. There has been little revision of the Orders or Manual that reflect technology advances (e.g., the fact that a single electronic media item can contain vast quantities of information, equivalent to thousands of documents). The Secretary's June 19, 2000 enhancements establishes a requirement for implementing encryption of certain high-density media, increased security requirements for certain classified data bases, and a DOE-wide inventory of electronic media that contains certain information. LLNL and SNL-NM are working aggressively to implement this new direction. Continued interaction between the NNSA/DNS and the laboratories will be needed to achieve implementation.

(U) The inconsistent approaches and levels of effectiveness described above are by-products of the lack of specificity and minimal standards in DOE orders. In the absence of specific requirements, sites have too much flexibility to interpret the requirements and will often make security decisions based on operational convenience and available facilities, equipment, and resources.

(U) Compounding the lack of specificity in certain areas is the historically slow response from SO and its predecessor organizations. For example, SNL-NM has been implementing manpower-intensive compensatory measures since the July 1999 Independent Oversight inspection while awaiting SO guidance related to protection of classified parts. Similarly, there is insufficient DOE guidance for identifying what information is SUCI Sigma 14. This is a longstanding policy issue and the subject of requests for clarification from several sites.

Lack of Direction on Implementation of the Need to Know Principle (U)

(U) DOE has a general policy that requires limiting information to those with a valid, job-related need to know. However, there are few standards and expectations for implementing a need to know program. The methods and effectiveness varied widely between the two sites and within the same site. In some instances, large vaults containing many types of information had no additional partitioning such that anyone with access to the vault would have access to any of the information therein, with no explicit provisions for need to know. In other cases, there were separately locked areas/safes containing information from particular programs. Similarly, there were different approaches for determining who

would be granted access on a need to know basis. For example, in some divisions, LLNL management made a blanket determination that everyone in the Division needed access to all information located in a large vault that had a wide variety of information on different programs. While a questionable practice, there are no specific provisions in the DOE order that explicitly preclude such a practice. Conversely, there were instances where the controls on need to know were very tight with only a very few authorized users and stringent procedures for granting access to information to other personnel who may need the information.

Over-Reliance on Individual Compliance (U)

(U) Protection against the insider is the most challenging part of information security. Certain personnel need access to information to do the job we pay them to do – such as designing nuclear weapons and serving on NEST teams to respond to a nuclear emergency. DOE has a personnel security program that requires all personnel to undergo background investigations and receive a Q clearance before being granted access to Secret Restricted Data. DOE also has programs, such as training and security awareness programs, that are intended to ensure that personnel are aware of their security responsibilities.

(U) No program, however, can provide full assurance against the determined insider, especially one that willingly disregards or circumvents procedures. If an individual has access to information, it can be compromised by various means, such as removing the materials, creating copies, or simply telling unauthorized personnel. Similarly, information can be compromised by careless mistakes, such as leaving documents unattended. DOE policy recognizes that some level of risk is inherent when individuals are allowed access to information and that the possibility of a trusted and authorized individual performing acts of espionage cannot be fully precluded.

(U) In addition, DOE sites must be vigilant to ensure compliance with DOE requirements. In any organization, especially ones that place a high value on the open exchange of ideas as an operational necessity in a research and development environment, there are likely to be individuals that view security measures as overly restrictive and will be tempted to disregard or shortcut requirements. The potential for such actions is heightened if requirements are not practical or require use of arcane technology or approaches (as has sometimes been the case). Such pockets of resistance to security are a continuing concern at the national laboratories and will continue to be an area that requires attention for the foreseeable future. The national laboratories, particularly LANL and LLNL which are operated by a university, have a historical reputation of tolerance for non-compliance with procedures. However, the results of the 1999 Independent Oversight reviews and this special review indicate that, as a result of the previously discussed Secretarial initiatives and attention, senior managers at the laboratories are actively involved in promoting security and that security is receiving considerable support. Changing a "site culture" is a significant challenge and a long-term undertaking that requires continued and proactive management support and involvement, as well as clear and demonstrated individual and organizational accountability for compliance.

(U) Although progress is being made, DOE laboratories are still vulnerable to the actions of a single individual who is authorized access to sensitive classified information. For example, at LLNL and SNL-NM as well as most other DOE sites, there are few measures that would prevent individuals from making unauthorized copies of classified documents, including accountable documents. There are few provisions for random checks/searches of personnel or areas to determine if documents/items are being used and stored as required (e.g., to determine whether individuals are violating security procedures by storing classified documents in desk drawers). DOE laboratories rely primarily on compliance with

DOE requirements and have not consistently and systematically attempted to identify and implement prudent measures that could reduce risks. The results of the reviews of LLNL and SNL-NM indicate that there are opportunities to further reduce risks by judiciously applying prudent measures like application of a two-person rule for certain activities, such as protection of high-density information on computer media.

(U) DOE has personnel security programs in place to lesson the risk of an insider and security awareness programs to encourage attention to security. The reduction in other security measures (e.g., the elimination of accountability requirements for Top Secret matter) places increased emphasis on the personnel security program component.

(U) With some exceptions, DOE's human reliability programs do not currently encompass any classified information activities regardless of the sensitivity of the information (exceptions include those that also involve special nuclear material and downloading of unclassified information from classified computers). As part of the ongoing effort to revise 10 CFR 710 Subpart B and combine the PSAP and PAP into a single program, DOE is currently working to establish requirements and criteria for including personnel with access to certain types of information in the human reliability program. Also, DOE has recently initiated polygraph examinations for certain categories of employees that have access to sensitive classified information.

Inadequate Definition of the Graded Approach (U)

(U) DOE has a provision requiring a graded approach to protection of classified matter. The concept of a graded approach is appropriate; certain types of classified matter are more sensitive and warrant higher levels of protection than other types. However, the guidance related to the graded approach is minimal, consisting of only a few paragraphs of general guidance and examples that cite broad categories of information (e.g., "information useful in developing a nuclear weapon"). The guidance is not sufficient to allow sites to determine how to categorize security interests in a manner that would allow a graded protection strategy. Also, it does not include a methodology for identifying progressively higher levels of security.

(U) LLNL and SNL-NM each have some examples of implementing measures beyond those specific minimum mandates, such as tracking systems for documents. However, neither LLNL nor SNL-NM has a systematic method for implementing a graded approach. The examples in which additional measures are implemented largely reflect a piecemeal application of professional judgment and resource and equipment availability rather than a systematic, top-down approach that involves defining policy, establishing protection objectives and requirements, and then determining resources needed to meet the requirements.

(U) In general, the classified matter protection Manual places the onus on line management and the field to develop and justify a graded approach. According to the Manual, the Heads of Departmental Elements are required to provide a risk-management-based framework for making security-related decisions and the sites are required to develop plans that describe, justify, and document the graded protection approach. Although this delegation of responsibility provides flexibility to the field, it has not proven effective. For LLNL and SNL-NM, the Head of the Departmental Element has historically been the Office of Defense Programs and, since March 2000, has been the Administrator of the National Nuclear Security Administration (NNSA). Neither the Head of the Departmental Elements nor the respective operations offices (AL for SNL-NM and OAK for LLNL) have provided formal direction for implementing a risk-based approach. The laboratories have little in their security plans about a graded approach for protection of information.

(U) Further, DOE policy currently does not provide sufficient guidance to enable sites to systematically and consistently identify the assets that warrant additional protection. Other than the classification levels and categories (Confidential, Secret, and Top Secret, and Restricted Data, Formerly Restricted Data, and National Security Information) and certain special information (a few documents are identified by Sigma subcategories), there is little policy for establishing the relative importance of various types of information. There are two significant problems that need to be addressed in this regard:

(U) Currently, the Secret Restricted Data category covers a wide range of information, some of which is particularly sensitive. However, the protection requirements for Secret Restricted Data matter in DOE orders make no distinction between the highly sensitive Secret Restricted Data (such as use control information and design of the most advanced nuclear weapons) and information of lesser sensitivity. DP and SO have attempted to work with DoD to assign higher classification levels (Top Secret) to certain types of data, particularly high density electronic media that include large amounts of data related to nuclear weapons systems design and testing (encyclopedic data). What is needed is a clear set of criteria for determining which information requires enhanced protection and a corresponding set of standards for protection measures. Such criteria should consider factors such as the subcategory of the information (e.g., Sigma level), the density of information (large amounts of data on a single media item would require additional protection), the value of the information to an adversary, comprehensiveness (documents with complete design information for a weapon system should receive additional protection) and other such factors.

(U) Although there are some differences (e.g., storage and transmittal), the minimum protection requirements for Top Secret are not significantly more stringent than those for Secret or Confidential. According to DOE orders, Top Secret could be stored in a GSA-approved security container anywhere in a limited area, with no requirements for alarm protection or protective force patrols, as long as the container has a specific type of lock. These minimum requirements are not much different than those for Secret; the only difference being that Secret would only require a standard combination lock. As currently defined, these minimum requirements provide only slightly more protection to the higher value Top Secret matter (the loss of which could cause "grave damage" to the national security). An effective graded approach needs to identify a progressively more stringent set of controls (addressing logs, need to know, access controls, encryption, and other measures in addition to storage).

(U) Overall, the graded approach is not adequately defined and does not provide sufficient guidance to facilitate effective implementation by DOE sites. The Secretary of Energy, in his June 19, 2000 memorandum, has outlined certain immediate and near-term measures and the NNSA/DNS has developed implementing guidance. These measures are consistent with a graded approach in that they identify specific actions for certain types of classified matter. While an appropriate interim step, the longer-term approach needs to address other repositories in addition to vaults and needs to include practical guidelines related to categorizing the relative importance of security interests.

10 Conclusions and Recommendations (U)

(U) In general, LLNL and SNL-NM meet the minimum DOE requirements for control of classified matter in the areas reviewed by the Independent Oversight team. While some specific improvements are warranted, no significant unmitigated deficiencies were identified. However, the current requirements for controlling classified matter are not as stringent or clear as needed in light of DOE's

particularly sensitive nuclear-weapons-related information. Improvements to policy are needed to ensure that DOE expectations are clearly defined. Particular attention is needed to more clearly define protection requirements in areas such as need to know and establishment of a graded approach that are clearly understood and can be effectively implemented to enhance protection of DOE's most critical assets.

(U) Appendices B and C provide specific opportunities to improve the classified matter protection programs at SNL-NM and LLNL, respectively. This section provides Independent Oversight recommendations for actions to be taken by DOE Headquarters to improve DOE policy. In developing the recommendations below, Independent Oversight recognizes that the NNSA/DNS developed guidance for implementing the Secretary's June 19, 2000 direction to enhance protection measures. NNSA/DNS is working with the field to ensure that questions are resolved and additional guidance is developed as needed. Independent Oversight believes that the enhanced protection measures and the recent implementing guidance provide a good framework for improving protection on an immediate and near-term basis. The recommendations below are intended to complement the recent direction and implementing guidance by identifying additional areas that should be considered for near-term and longer-term action.

1. (U) **Re-institute requirements for a formal accountability system for certain types of information.** The current requirements for accountability need to be strengthened and clarified. Top Secret and Secret Restricted Data related to nuclear weapons should be included. An evaluation should be conducted to determine whether other Secret Restricted Data (related to production of special nuclear materials and nuclear energy) should be included. Various methods to apply commercially available technologies (e.g., databases, bar codes, using badge swipes to check out documents) should be explored to facilitate implementation and make the system user friendly and useful for operations as well as security (e.g., data searches and data mining). Lessons learned from sites currently using accountability systems should be solicited and utilized to facilitate the reinstatement of formal accountability.

2. (U) **Establish a clear and comprehensive graded approach and issue appropriate implementing guidance.** An effective graded protection approach needs to incorporate additional measures for accounting for and tracking the more sensitive types of documents/items, including more stringent measures for controlling and recording access to repositories. The recent Secretarial direction for enhanced protection measures and NNSA/DNS implementing guidance provide a good start. This initiative needs to be expanded to include other storage repositories (in addition to vaults). It also needs to include practical guidelines for categorizing the relative importance of security interests, and include a methodology for systematically identifying priorities and protection measures for various types of security interests.

3. (U) **Clarify the need to know policy.** Clear policy and criteria are needed to ensure that DOE sites strengthen implementation of the need to know principle. Specific areas that need to be addressed are expectations for partitioning information within large storage areas and prudent measures to restrict access to those with a specific need to know (rather than unilateral decisions that an entire Division has a need to know all information in a vault or program).

4. (U) **Continue efforts to expand the human reliability programs.** The ongoing NNSA/NSD effort to include personnel in positions with access to certain types of nuclear weapons information are noteworthy and should be finalized and implemented. DOE's graded approach should explicitly consider participation in

the human reliability program as a control in a graded approach to protection. The parameters of the program should also be re-evaluated to ensure that it is designed to provide assurance of an individual's trustworthiness (e.g., polygraph examinations).

5. (U) **Conduct a review of special access programs and sensitive compartmented information.** These program include highly sensitive information and only a few individuals are authorized access to areas where special access programs are conducted or to sensitive compartmented information facilities. These programs should be reviewed in a manner similar to this review, either by the Office of Independent Oversight and Performance Assurance or the organizations that are responsible for direction and oversight of sensitive compartmented information and special access programs.

6. (U) **Develop a plan and milestones for revising and reissuing the DOE orders and manual to reflect recent and planned policy changes.** The changes directed by Secretary Richardson and further defined by the NNSA/NSD need to be refined and then incorporated into the applicable DOE orders and manuals (those for classified matter protection and computer security) on an expedited basis to ensure that they are institutionalized and incorporated into contracts with DOE site contractors. Other modifications to the classified matter protection order and manual, such as clarifying requirements for a graded approach, need to know, and accountability, should also be made as soon as possible. Also, SO should accelerate efforts to develop and issue guidance regarding the protection of classified parts.

REDACTED VERSION

APPENDIX A (U)

The Office of Independent Oversight and Performance Assurance (Independent Oversight) is charged with the independent oversight of safeguards and security programs within the DOE. Independent Oversight's independence is assured by its organizational placement directly under the Office of the Secretary of Energy. Independent Oversight performs its reviews in accordance with DOE Order 470.2A, *Security and Emergency Management Independent Oversight and Performance Assurance Program*. This order establishes the foundation for the independent evaluation of the effectiveness of DOE safeguards and security policy and programs, and the implementation of those policies and programs.

The Independent Oversight team composition follows:

Office of Independent Oversight and Performance Assurance (OA-1)

Glenn Podonsky, Director
Mike Kilpatrick, Deputy

Office of Safeguards and Security Evaluations (OA-10)

Barbara Stone, Director
John Hyndman, Deputy Director

Independent Oversight Review Team Management

Glenn Podonsky, Overall Team Leader
Mike Kilpatrick
John Hydman

Independent Oversight Team at Lawrence Livermore National Laboratory (LLNL)

James Taylor, Team Leader at LLNL
James McGee
Steve Crowe
Richard Donovan
John Easterbrooks

Independent Oversight Team at Sandia National Laboratories-New Mexico (SNL-NM)

Pete Rodrik, Team Leader at SNL-NM
Ralph Kurtzman
Mike Stalcup
Jerry Bennett
Ken Jurjevich

Administrative and Quality Support

Dean Hickman
Tom Davis
Margaret Stroud
Leisa Weidner

Information on this page is Unclassified.

REDACTED VERSION

REDACTED VERSION

APPENDIX B (U)

CONTROL OF CLASSIFIED WEAPONS DATA AT SANDIA NATIONAL LABORATORIES-NEW MEXICO (U)

B.1 INTRODUCTION (U)

(U) As directed by the Secretary, the Office of Independent Oversight and Performance Assurance (Independent Oversight) conducted a Special Review of the effectiveness of management efforts to implement classified matter protection and control procedures for classified weapons data at Sandia National Laboratories-New Mexico (SNL-NM). The review was conducted from June 17-23, 2000. The Special Review focused on the administrative controls in place to protect weapons data, including use control and Top Secret information. Consequently, data collection activities were conducted primarily in two SNL-NM organizations where such information is concentrated: the Weapons System Center (2000) and the Manufacturing Systems, Science and Technology Center (14000).

(U) Data collection activities included interviews of managers and staff responsible for protecting classified information, reviews of policies, procedures and other documents associated with controlling and protecting classified information, examinations of classified matter storage facilities, observation of document control procedures and practices, performance testing of accountability systems, and examination of classified documents. A selection of line managers in the focus organizations (2000 and 14000) were interviewed to determine their levels of involvement and their management actions to implement classified information protection requirements. Document custodians in the same organizations were interviewed to ascertain their level of pertinent knowledge and to verify their document control procedures. Managers with programmatic responsibilities for safeguards and security were interviewed to ascertain broader aspects of program implementation, trends, and support.

(U) As evidenced by the results of this review, SNL-NM has demonstrated strong management involvement in efforts to protect classified weapons data in its custody. While additional management attention is warranted in a few areas, SNL-NM is adequately implementing requirements for the protection and control of classified matter.

B.2 STATUS AND RESULTS (U)

Background (U)

(U) Two SNL-NM initiatives with significant impact on the protection of classified matter were underway prior to this Special Review. First, as the result of an SNL-NM reexamination of their security program following the 1999 Independent Oversight comprehensive inspection, significant changes in their approach to security management and implementation have been underway during the past eighteen months. The thrust of the initiative is to employ an integrated security management model that shifts primary responsibility for implementation of security requirements from safeguards and security program managers to line managers who possess the assets requiring protection. The implementing vehicle, the Laboratory Management Program for Integrated Security (LAMPIS), is in the final stages of approval.

REDACTED VERSION

(U) Second, in direct response to the security incident at Los Alamos National Laboratory involving Nuclear Emergency Search Team classified hard drives, SNL-NM took several actions involving classified computer equipment and media maintained for off-site emergency response by members of the Accident Response Group (ARG) and the Joint Technical Operations Team (JTOT). These actions, begun on June 14, 2000, included: establishing an issues management team to ensure an integrated, proactive, effective response; inventorying and placing classified hard drives and CD-ROMs containing compendia of weapons information into accountability; placing those same items under two-person control; and instituting check-in/check-out requirements and weekly and unannounced inventory requirements for those items. (The classified hard drives were placed into accountability approximately one year ago).

(U) In the context of a situation in which many of the activities associated with the two initiatives were still in progress, the review team developed the following information relative to the status of SNL-NM management's implementation of classified matter protection requirements.

Line Management Responsibility for Safeguards and Security (U)

(U) Although not all actions associated with the transition to the integrated security management system are complete, the fundamental change that places responsibility for the implementation of security requirements on line managers has been promulgated through corporate (laboratory) policy and is understood and accepted by line managers. SNL-NM has demonstrated high-level support for security by appointing the Vice President for Laboratory Services the Chief Security Officer and assigning line managers responsibility for implementing security requirements in their organizations. Results of interviews with line managers at every level indicate they clearly understand that they are responsible for controlling and protecting the classified assets possessed by their organizations, and that they must do so in accordance with established DOE and laboratory policies and procedures. As line managers, they have the authority to ensure that this is accomplished within their organizations. This understanding and acceptance of responsibility was confirmed through observations and discussions with other line managers and staff during visits to organizational Document Control Stations and classified information storage locations. Further, performance evaluations of line managers and their staff members include evaluation of performance in this area (security responsibilities).

(U) Line managers indicated that they have sufficient senior management support, including adequate resources, to accomplish their security-related responsibilities. This perception is supported by such evidence as a laboratory-wide large-scale procurement of GSA-approved security containers and the construction of additional vault-type rooms to replace substandard storage containers (e.g., space-saver cabinets) formerly used to store many classified documents. In addition to senior management support, line managers indicated that their organizations have a good working relationship with and receive adequate support from the Classification and Information Security (7121) organization. For example, if they have a question regarding the handling, storage, or processing requirements for a particular classified document, they can and do ask for and receive the necessary support from the security specialists in organization 7121.

(U) SNL-NM management has, in its internal website, an effective vehicle for laboratory-wide dissemination of requirements and other information (e.g., bulletins) associated with the protection of classified matter. The two currently effective laboratory procedural manuals dealing with the protection of classified documents and materials both date from 1996; the DOE policy they implement dates from 1999. A new revision of the procedure covering document control is ready for comment. The procedure addressing classified materials control is next in line for revision. Although both current procedures are outdated in that they predate by several years the DOE guidance they are intended to

implement, the practical effects of this situation on the protection of classified matter are minimal, since the current DOE guidance did not significantly change previous guidance, and, more importantly, did not increase protection requirements.

Personnel Competence and Training (U)

(U) Results of review activities indicate that classified document custodians are competently performing their duties. Interviews of custodians revealed, in every case, a comprehensive knowledge of laboratory requirements and organizational procedures for all pertinent aspects of classified document handling and control. Upon initial assignment as a Classified Document Custodian, individuals are certified through completion of a five-day training course, discussed below. Periodic re-certification is not required. All custodians interviewed indicated they had completed the course.

(U) Interviews and observations of line managers, as well as observations and incidental discussions with other staff members, indicated that those individuals are familiar with and properly perform classified document control procedures. Staff members who handle classified information are required to read and comply with document control requirements and procedures; while they receive general security awareness training; they are not required to attend the formal training that custodians must attend.

(U) SNL-NM's formal training course for classified document custodians is designed to provide a basic understanding of the procedures associated with protecting, controlling, generating and marking, storing, transmitting and receipting, destroying, and controlling access to classified information. It includes lectures, practical exercises, and tests. SNL-NM could not describe the genesis of the course, or whether it had been based on a job-task analysis. The training is presented by instructors from the Classification and Information Security Department (7121), none of whom have attended the NNSI instructor certification course. Although, upon course completion, attendees are provided certificates of competency, no central record is maintained to document attendance. Consequently, it is very difficult to determine who has completed the course or when. Regardless of these few apparent weaknesses in the formal training course, the document custodians observed, most of who have been custodians for many years are sufficiently knowledgeable to perform their custodial duties competently.

Comprehensive Requirements (U)

(U) SNL-NM is effectively implementing DOE requirements for the protection of classified matter. In some instances, the laboratory has instituted additional protection measures that exceed DOE requirements. For example, the laboratory has retained full accountability for Top Secret matter, even though all Top Secret documents are stored in GSA-approved security containers within vault-type rooms located in a Limited Area. Additionally, the laboratory has recently created accountability, inventory, and two-person physical control procedures for classified disk drives and CD-ROMs containing information used by the ARG and JTOT for emergency response.

(U) The laboratory has implemented standardized procedures and other guidance for controlling classified matter, and has made them easily available to all employees by placing them on-line on the laboratory's internal network. The laboratory-wide procedures provide sufficient detail to assist and enable users to comply with DOE and laboratory requirements. Security specialists in organization 7121 or division security coordinators provide additional guidelines, details, or explanations on request. Organization-specific implementation details are published by each Department in organizational security plans. As mentioned previously, the laboratory-wide procedural manuals are dated and require

revision; the document control manual revision will be released for comment next month, and the material control manual revision is planned.

[REDACTED PARAGRAPH]

(U) Access lists are maintained for all classified repositories and for some specific types of information, such as Sigma 14 or Special Access Program information. Access is based on a need-to-know determination, which is normally made by the information "owner," usually the department manager. Need-to-know determinations vary depending on the manager's perceived organizational needs. In some organizations, virtually all staff members are granted access to all classified information in the organization's possession. In other organizations, access to information – particularly program-specific information – is granted only to staff working on the specific program to which the information applies. The need-to-know determinations are important, because those who have been certified and placed on the access lists typically have the repository combinations and free and full access to all information in the repositories. Organizations possessing Sigma 14 Sensitive Use Control Information store that information separately and make specific need-to-know determinations for that information, and may restrict repository combinations to a few individuals on the access list. Organizations possessing information they do not "own" – such as the image management center that stores drawings in electronic form – typically release classified information only to the data owner (e.g., program manager) or to individuals for whom the appropriate program manager has verified a need-to-know. A limited number of senior laboratory managers can grant access to Top Secret; specific need-to-know must be certified for each Top Secret document to be accessed. Laboratory management has recognized the sensitivity and critical importance of need-to-know determinations in the overall information protection effort, and is involved in an effort to identify a better system to apply need-to-know decisions to individual data.

(U) Generally, access to open repositories in organizational office spaces or vault-type-rooms is controlled either by keypad locks or by observation at the entry point. While staff members with approved routine access to the space (on the access list) have access to open repositories; visitors who enter the area are escorted. In some organizations, repositories (generally GSA-approved safes) are kept locked, and opened only long enough to retrieve or replace a document. Once the security lock to a vault-type room is unlocked, a keypad lock still secures the door. Personnel with routine authorized access to the vault-type room can enter using the keypad. Visitors (those not having routine access) must be escorted and must log in and out. Since some organizations do not yet have sufficient numbers of GSA-approved safes or vault-type rooms, some information belonging to several organizations is currently being commonly stored in vault-type rooms. In these cases, organizations maintain need-to-know access control over their information by storing it in locked space-saver cabinets (within the vault-type rooms).

(U) As of the date of data collection, a day-lock procedure allowed classified to be left in open storage in unattended vault-type rooms under keypad lock control (security combination lock open, alarms off) for up to an hour. Changes in this practice resulting from Secretarial guidance are discussed at the end of this section.

(U) Systems used to account for Top Secret and Sigma 14 documents were examined, and performance tests were conducted to see if custodians could locate and produce a sample of documents

selected from the accountability records. All accountability systems and records were complete and 7accurate, and all documents requested were produced.

(U) The laboratory's procedures for origination, transmittal, reproduction, and destruction of classified fully comply with requirements. Classified document custodians verify markings, conduct any necessary document reproduction on approved copy machines, and handle all receipts and transmittals. Custodians destroy documents using shredders available in organizational offices, or use burn bags for removal and destruction at central destruction facilities. When accountable matter (e.g., Top Secret, Sigma 14, etc.) is destroyed, certificates of destruction are generated and a cleared person witnesses the destruction. Central destruction facilities include shredders, macerators, disintegrators, degaussing units, and smelters. Two Q-cleared individuals witness destruction of classified matter at the central facility.

[REDACTED PARAGRAPH]

(U) In response to deficiencies in the storage of classified material identified by Independent Oversight during the 1999 Comprehensive Inspection, a number of compensatory measures were put in place and upgrades planned or made. An Independent Oversight Follow-up Review in December, 1999 found some compensatory measures (e.g., protective force personnel posted after hours) still in place, pending guidance from SO regarding non-standard storage of classified matter. That guidance has not been forthcoming, and some compensatory measures remain in place, almost a year after the problems was identified.

Feedback and Improvement (U)

(U) SNL-NM does not currently have a fully functioning comprehensive self-assessment process that encompasses the classified matter protection and control program. Until the fall of 1999 a multi-tiered program of self-assessments was in place. It included ongoing audits of classified document and material control stations by safeguards and security personnel, an annual CMPC programmatic self-assessment, and a CMPC component of an annual safeguards and security program self-assessment.

(U) In the fall of 1999, a decision was made to reorganize and restructure safeguards and security at SNL-NM, placing program implementation in the hands of line managers. At that time, the existing audit program was discontinued, and no audits have been conducted to date. The CMPC Team Leader completed an internal self-assessment in March 2000, identifying two deficiencies: the need to update CMPC procedures; and the need to improve document custodian training. No document or material control stations were examined in connection with this self-assessment.

(U) One result of the reorganization of the safeguards and security program was the development of a new audit/self-assessment program that is to be managed by the S&S/ES&H Reporting and Feedback Department (7112). The new CMPC assessment program is scheduled to begin in September 2000. Important aspects of the new program include: self-assessments of document control stations will be conducted by line organizations, with assistance as required from the CMPC Team; and the CMPC

Team will conduct random audits of document control stations based on security holdings and past performance, and will look at additional areas such as classification, OPSEC, and portions of physical security systems. The new program contains all the elements typical of a comprehensive self-assessment process, and, if effectively implemented, should provide adequate information to managers concerning program status.

(U) Self-assessment activities are handicapped by the fact that the CMPC Team auditors, while having Q clearances and access to all Sigmas, do not have SCI access or access to special access programs. Consequently, they cannot assess the adequacy of the entire CMPC program. Though future self-assessments will be conducted by line organizations whose members have the necessary access, the lack of access will continue to restrict the effectiveness of that part of the program consisting of random audits by CMPC Team personnel.

(U) The last security survey conducted by the Albuquerque Operations Office that included the CMPC topic dates from 1997. No survey was conducted in 1999 due to a Comprehensive Inspection and a Follow-up Review conducted by Independent Oversight. A security survey is scheduled for July 2000.

(U) SNL-NM has a system to prioritize and track security deficiencies. Corrective action plans are developed to address deficiencies identified by outside inspections or surveys or by the Self-Directed Assessment. In those cases, the responsible organization determines if a root cause analysis is needed. However, no criteria are provided to determine when a root cause analysis is needed. In the future, it is anticipated that corrective action plans will be developed for deficiencies detected during self-assessments and random audits that cannot be corrected on the spot.

(U) The laboratory has a recent history of correcting deficiencies in a timely manner. For example, all findings from the 1999 Independent Oversight inspection were closed by AL by January 2000. (However, due to the limited scope of this Special Review, Independent Oversight did not verify the adequacy of all corrective actions).

Response to the Secretary's Enhanced Protection Measures Requirements (U)

(U) On June 21, 2000, SNL-NM managers indicated that their immediate response to points 3 and 4 of the Secretary's Memo of June 19, 2000, "Enhanced Protection Measures," will be implemented at start of business on June 22, 2000 and are as follows:

(U) Log-in log-out procedures will be used for all vaults and vault-type rooms to record each entrance and exist by all personnel, whether routinely authorized or a visitor. An example log sheet was provided.

(U) All vaults and vault-type rooms must be attended by an authorized person at all times or placed in a "locked (by spin-dial combination) and alarmed" state. "Attended" means that the access/egress point for the vault must be under continuous, positive control by a person authorized access to that specific vault, or the vault must be occupied and an electronic access control system is controlling access for authorized personnel. Current procedures allowing the use of day-locks for protection of unattended vaults are immediately suspended.

(U) SNL-NM will await further implementation guidance from SO before implementing the remaining points, as indicated in the Secretary's Memo. However, it is noted that SNL-NM has already

addressed one additional point through previous actions, as described at the beginning of this section, to account for and inventory certain computer media maintained for ARG/JTOT emergency response.

B.3 CONCLUSIONS (U)

(U) Overall, SNL-NM is adequately implementing requirements for the protection and control of classified matter. In some cases laboratory practices utilize a graded approach; such as their practice of accounting for Top Secret matter and their recent enhancements to account for, frequently inventory, and exercise two-person control over certain computer media maintained for emergency response purposes. There is ample evidence that a major programmatic reorganization aimed at placing responsibility for security in the hands of line managers is gaining acceptance and taking hold in line organizations. This and other initiatives reflect significant senior laboratory management support for safeguards and security.

(U) Implementation of protection requirements at the user organizational level is generally effective. Personnel responsible for controlling classified documents demonstrated clear understanding of their responsibilities and the required procedures, and had the necessary resources available. Need-to-know decisions are made at the (usually) Department-level, based on the managers' need to balance work requirements with the need to restrict access as much as possible. The laboratory has completed a significant effort to store all classified documents in an approved manner, utilizing approved security containers. However, compensatory measures remain in place at some non-standard storage locations for classified parts.

[REDACTED PARAGRAPH]

(U) Although ongoing initiatives and resolution of some pending issues remain to be completed, SNL-NM is effectively implementing protection requirements for classified matter and is currently guiding its protection program on an upward, improving course.

B.4 OPPORTUNITIES FOR IMPROVEMENT (U)

(U) The following items have been identified as potential enhancements to the existing programs. They are not intended to be prescriptive in nature; rather, they are intended to be reviewed and evaluated by the responsible DOE and contractor line managers, and prioritized and modified as appropriate in accordance with site-specific programmatic and safeguards and security objectives.

- (U) Consider having skilled systems personnel conduct detailed testing of motion detectors in vault-type rooms, as they are currently configured, to determine the adequacy of sensor coverage.
- **[REDACTED PARAGRAPH]**
- (U) Consider the need to conduct, without delay, audits of document control stations with the most sensitive holdings, with histories of weak performance, or with newly assigned custodians.

- (U) Consider the value of granting CMPC Team members who conduct audits access to the SCIF and to Special Access Programs for audit purposes.
- (U) Establish criteria to guide responsible managers in determining when root cause analyses are needed for internal and external findings.
- (U) Consider the benefits of upgrading the formality of the document custodian-training course by basing it on a job-task analysis, providing the instructors with formal training, and maintaining training records.

REDACTED VERSION

APPENDIX C (U)

CONTROL OF CLASSIFIED WEAPONS DATA AT LAWRENCE LIVERMORE NATIONAL LABORATORY (U)

C.1 INTRODUCTION (U)

(U) This review of the effectiveness of Classified Matter Protection and Control (CMPC) procedures at the Lawrence Livermore National Laboratory (LLNL) was conducted from June 17 through June 23, 2000. The review focused on the protection of the most sensitive classified assets at the Defense and Nuclear Technologies Directorate (DNT), such as weapons design information and use control information. Within this scope, key aspects of protection, including generation, storage, marking, destruction, and control of access to such materials were examined. Particular attention was devoted to the role of laboratory management in ensuring that DOE policies related to control of classified matter are established and implemented within the laboratory divisions selected for review.

(U) Data collection activities included interviews with managers and staff responsible for protecting classified information, reviews of policies, procedures and other documents associated with controlling and protecting classified information, examinations of classified matter storage facilities, observation of document control procedures and practices, performance testing of control procedures, and examination of classified documents and computer media. The scope of this review was generally limited to DNT. However, LLNL Top Secret accounts and the Sigma 14 and 15 weapons data account (not a responsibility of DNT) were reviewed as well. Cognizant line managers for these accounts were interviewed to determine their levels of involvement and their management actions to implement classified information protection requirements. Document custodians and computer systems administrators with responsibilities for these accounts were interviewed to ascertain their level of pertinent knowledge and to verify their document control procedures.

(U) As evidenced by the results of this review, LLNL has demonstrated strong management involvement in efforts to protect classified weapons data in its custody. While additional management attention is warranted in a few areas, LLNL is adequately implementing current DOE requirements for the protection and control of classified weapons data.

C.2 STATUS AND RESULTS (U)

Background (U)

(U) Two LLNL initiatives with significant impact on the protection of classified weapons data were underway prior to this review. In response to the security incident at Los Alamos National Laboratory involving Nuclear Emergency Search Team (NEST) classified hard drives, LLNL commissioned a committee on June 15, 2000, to evaluate all vaults and vault-type rooms at LLNL. The focus of this committee's efforts is 1) to determine any vulnerabilities or other concerns that may exist, 2) to construct a self-assessment check list to be used by custodians to gather and evaluate status, and 3) to produce a listing of assessments and training currently deployed. This effort is proceeding rapidly. A self-assessment checklist has been prepared and distributed to custodians. Their reply was due during the week of June 19, 2000. No results were available at the time of this review, although the self-assessment check sheet was reviewed and appeared to be comprehensive.

REDACTED VERSION

REDACTED VERSION

[REDACTED PARAGRAPH]

Line Management Responsibility For Safeguards And Security (U)

(U) DNT is administratively responsible for personnel assigned to the two divisions responsible for nuclear weapons primary and secondary design and the division responsible for Inertial Confinement Fusion (ICF) design. DNT also administers the two classified library vaults in which a large amount of nuclear weapon design and testing data resides, as well as one classified computer network containing much of this data in electronic form. The Associate Director for Defense and Nuclear Technologies is also responsible for LLNL's activities under the Stockpile Support Program, which involves matrixed personnel not administratively assigned to DNT. This program represents almost 50 percent of LLNL's budget and personnel resources and involves many personnel not administratively assigned to DNT. Therefore, line management responsibility for the majority of the most sensitive weapons data held by LLNL flows from the Oakland Operations Office through the Laboratory Director to the Associate Director for Defense and Nuclear Technologies.

(U) LLNL also has a CMPC Manager who heads the Classified Document Project Office (CDPO). This project office, established in 1991, provides programmatic direction and oversight to the LLNL CMPC program. Specific activities include interface with all levels of LLNL management, ensuring development of LLNL CMPC procedures, developing and implementing CMPC training for custodians and Classified Administrative Specialists, performing CMPC self-assessments, and managing the Livermore Administrative Document System (LADS).

[REDACTED PARAGRAPH]

(U) CMPC program requirements for Special Access Programs (SAPs) and Sensitive Compartmented Information Facilities (SCIFs) are under the purview of DOE Headquarters activities and are not generally administered or overseen by the LLNL CMPC Manager or the CDPO. Therefore, while the LLNL organizational structure generally facilitates efficient and effective communication and working relationships among those who use and generate classified matter, communication and working relationships between those involved with SAPs and SCIFs and the remainder of the CMPC program are less efficient.

REDACTED VERSION

REDACTED VERSION

(U) Position descriptions of DNT personnel generally include their responsibilities for the CMPC program and for protecting classified matter. These elements are considered during performance and salary reviews. DNT managers cited examples in which evaluations of an individual's effectiveness in addressing their responsibilities for protecting classified matter have affected their performance ratings and therefore influenced managers' decisions regarding promotion and salary increases.

(U) LLNL line management is involved in and actively supports the CMPC program in DNT. They have provided the management support needed by the CMPC manager to administer the CMPC program. In response to recent events, they have initiated and supported efforts to provide graded levels of protection for selected classified matter. LLNL line management has shown that they understand and accept their responsibilities for the security of classified matter.

Personnel Competence And Training (U)

(U) In each of the storage locations visited during this review, personnel responsible for access control of the area and control of the classified matter in the area were interviewed to determine their familiarity with DOE order requirements and local requirements and procedures. In every case, personnel demonstrated a comprehensive knowledge of requirements and procedures, including the newly instituted enhanced chain of custody procedures. Line managers interviewed also demonstrated familiarity with requirements and procedures for protecting classified matter. Limited Scope Performance Tests indicated that custodians were adequately carrying out requirements for document marking, document transmittal, and document destruction.

(U) A review of the CMPC training program as implemented within DNT revealed that a set of formal training courses and briefings exists to meet the needs of all personnel working with classified matter. Each employee receives a comprehensive initial briefing upon obtaining an access authorization that includes their responsibility for protecting classified matter as well as specific procedures used at DNT to generate, use, store, transmit, and destroy classified material. In addition, each employee receives an annual refresher briefing. The training materials used for the initial and the most recent annual briefing were reviewed and found to be appropriate.

(U) In addition, CASs and document custodians receive additional formal training. Their training includes not only CMPC training, but also training in Operations Security (OPSEC), Technical Surveillance Countermeasures (TSCM), and classification procedures. These materials are also continuously available to personnel through a web-based intranet site. These training materials were reviewed and found to be consistent with current DOE policy and comprehensive. In addition, the CMPC manager has regularly scheduled meetings with CASs to communicate and discuss changes in policy or procedures.

(U) LLNL training programs and materials are adequate to meet the needs of those whose duties include handling classified materials. Interviews with DNT managers and staff revealed that these persons understood their responsibilities for protecting classified information and were knowledgeable of DOE, LLNL, and DNT requirements and procedures. Therefore, this review indicates that DNT personnel are competent to discharge their responsibilities for protecting classified information and that the training program is sufficient to maintain competency and bring new employees to a similar level of competency.

REDACTED VERSION

REDACTED VERSION

Comprehensive Requirements (U)

[REDACTED PARAGRAPH]

[REDACTED PARAGRAPH]

Access Controls (U)

(U) Access controls were generally found to be compliant with current DOE requirements. LLNL maintains access control lists for vaults and vault-type-rooms. Area custodians use these lists or personal recognition to determine who may enter without an escort. Access logs are kept for some types of activities – entry of non-division employees in one case and access to particular files in another. During working hours, access is controlled by area custodians, through the use of badge/card readers, or through the use of a day lock procedure when custodians are temporarily absent. During non-working hours, vaults and vault-type-rooms are secured and under intrusion alarm protection. Lock combinations are changed as required by DOE Orders.

[REDACTED PARAGRAPH]

[REDACTED PARAGRAPH]

REDACTED VERSION

REDACTED VERSION

[REDACTED PARAGRAPH CONTINUED]

[REDACTED PARAGRAPH]

(U) A third example is the use of access logs in vaults and vault-type rooms used to store classified material. While logs were in use at every location, there was little consistency in the requirements for logging or the information provided on the log. While there is no DOE order requirement specifying requirements for logging or the content of log sheets, a consistent requirement would provide a more reliable means of determining access to sensitive documents.

CMPC Procedural Requirements (U)

(U) Current site-wide procedures exist and fully comply with current DOE requirements. Observations at DNT accountability stations and storage areas indicated that these procedures were fully and effectively implemented. In most cases, written desktop procedures existed to assist personnel in addressing specific site-wide requirements and local requirements. Custodians interviewed quickly and effectively demonstrated their competence and knowledge. Limited reviews of document marking, document transmittal, and document destruction indicated that each was performed in accordance with DOE requirements.

(U) LLNL maintains the Livermore Administrative Document System (LADS) that is used to track access to selected documents. LADS provides LLNL staff with the means to determine who has had access or is allowed access to a given document, as well as providing other pertinent data. While DOE no longer requires that a unique identifier be applied to classified documents not under accountability, entry of a document into the LADS does include assigning an administrative identifier that can be used to identify the document.

(U) Review of the Top Secret accounts at LLNL indicated that all were operated in accordance with DOE policy and were appropriately safeguarded. In several instances, even though not required by DOE order, LLNL continues to maintain accountability records, and inventories had been conducted within the last two years. All Top Secret accounts are subject to annual self-assessment. Physical protection afforded Top Secret accounts is consistent with DOE requirements. Access to Top Secret documents is closely controlled and strictly limited by need-to-know. Custodians maintain current access rosters and effectively enforce access restrictions.

REDACTED VERSION

REDACTED VERSION

[REDACTED PARAGRAPH]

[REDACTED PARAGRAPH]

Feedback And Improvement (U)

(U) The primary mechanisms for management feedback regarding CMPC are the Oakland Operations Office Survey Program and the CMPC Manager's self-assessment program. Oakland Operations Office conducts survey activities throughout the year and consolidates the results in an annual report. There are currently no outstanding CMPC issues developing as the 2000 survey activities are being conducted. The results of the 1998 and 1999 Oakland Operation Office surveys were reviewed. Some CMPC findings were identified and Oakland Operations Office staff has worked with LLNL to resolve identified issues and bring the findings to closure.

(U) In early 1999, LLNL comprehensively revised its approach to the conduct of self-assessments. The new self-assessment program relies heavily upon questionnaires distributed to employees with classified holdings as a data source. The LLNL self-assessment program assesses areas of interest determined by the CMPC Manager at the rate of approximately one-third of all employees each year. Each selected employee completes the standard questionnaire and returns it to the CDPO. The CDPO staff reviews these questionnaires and combines the results with other data sources, such as a check sheet filled out by alarm technicians during periodic alarm tests. The CDPO staff analyzes these results to determine causal factors and to determine strengths and weaknesses of the overall CMPC program implementation. Summary analysis reports are prepared annually. The first report under the revised procedure is scheduled for September 2000. Reports may contain findings and observations designed to characterize areas in need of improvement. LLNL managers to whom findings are directed are expected to prepare and execute an effective corrective action plan. Closure of findings is validated by the CMPC Manager.

(U) Corrective action plans for the 1998 and 1999 Oakland Operations Office surveys were reviewed. All CMPC findings were adequately addressed and closed. Currently, LLNL has one open CMPC finding from the 1999 OA comprehensive inspection. This finding remains open and is shortly expected to be closed and validated by Oakland Operations Office. There are no open findings from the CMPC self-assessment programs.

[REDACTED PARAGRAPH]

REDACTED VERSION

REDACTED VERSION

[REDACTED PARAGRAPH CONTINUTED]

Response to the Secretary's Enhanced Protection Measures Requirements (U)

(U) A number of the efforts begun by LLNL in early June 2000 in response to the incident at Los Alamos National Laboratory have proven to be partially responsive to the Secretary's requirements. However, on June 21, 2000, LLNL had still not received an official copy of the Secretary's June 19th memorandum specifying enhanced protection measures for national security assets. LLNL managers had reviewed draft copies of the memorandum and had prepared a draft response pending receipt of the final memorandum. In that draft response, LLNL addressed both those items requiring immediate action and those with longer periods of implementation. Their draft response to immediate action items 3, 4, and 6 are discussed below.

[REDACTED PARAGRAPH]

C.3 CONCLUSIONS (U)

(U) LLNL has implemented a CMPC program that largely complies with DOE orders. Further, LLNL management has supported a proactive program of identifying especially sensitive information assets and providing enhanced protection for them. Personnel and managers with responsibilities for CMPC are knowledgeable, their position descriptions include their CMPC responsibilities, and their performance ratings include their effectiveness in performing CMPC-related duties. The CMPC training program is comprehensive and effective, and there are adequate training assets to prepare future employees for CMPC duties. The newly revised CMPC self-assessments represents a new approach with promise for enhancing the self-assessment program and providing meaningful management feedback concerning the CMPC program. LLNL has fully implemented two of the three security enhancements mandated as immediate by the Secretary in his June 19, 2000 memorandum and will complete the third by June 26, 2000.

(U) As evidenced by the results of this review, LLNL has demonstrated strong management involvement in efforts to protect classified weapons data in its custody. While additional management attention is warranted in a few areas (such as additional protection to certain back-up tapes, access controls, need-to-know determination, and consistency of procedures) LLNL is adequately implementing requirements for the protection and control of classified weapons data.

C.4 OPPORTUNITIES FOR IMPROVEMENT (U)

(U) The following items have been identified as potential enhancements to the existing programs. They are not intended to be prescriptive in nature; rather, they are intended to be reviewed and evaluated

REDACTED VERSION

by the responsible DOE and contractor line managers, and prioritized and modified as appropriate in accordance with site-specific programmatic and safeguards and security objectives.

- (U) Consider including some of the staff from SAPs and SCIFs in the periodic CAS meetings to exchange ideas and to achieve broader exposure to current areas of emphasis in CMPC.
- (U) Consider making common local procedures such as access logging more consistent.
- (U) Consider placing classified backup tape drives in which backup media remains for substantial periods of time in more secure containers and/or under continuous alarm coverage.
- (U) Consider using a project-oriented or task-oriented approach to determine need to know with frequent reviews to assure that need to know is consistent with current work responsibilities.
- (U) Consider additional reviews of information holdings to ensure that there are no other collections of data requiring enhanced protection measures. For example, consider whether there are highly valuable and portable data sources that are not particularly highly concentrated or whether there are some information assets whose value is so great that the portability of their container is a secondary issue.
-

Mr. COX. You have recommended that the human reliability program should be reevaluated to make sure that it is providing assurance of an individual's trustworthiness, and you specifically mentioned polygraphs for that purpose.

I take it it is your view that polygraphs are an integral part of the security function that you are trying independently to evaluate?

Mr. PODONSKY. As I answered in the last round of questions, yes, sir, we do believe that if it is applied in a reasonable way, that it can, in fact, be a way to enhance security.

Mr. COX. Are you troubled by the fact that it has taken so many years to get started?

Mr. PODONSKY. There are many things in the Department that trouble me, but this one in particular we haven't really focused on.

Mr. COX. I wonder whether I ought to address my questions next about changing the results of security surveys to GAO or to you, Mr. Podonsky?

Mr. PODONSKY. I am not familiar with how much GAO is cognizant of the survey program.

Mr. COX. Well, the Inspector General's report, of course, dated May 30, 2000, tells us that Department of Energy management changed ratings for the 1998 and 1999 surveys at Los Alamos without providing a documented rationale for the changes; that they did not fully address concerns about a compromise of force-on-force exercise; that they destroyed work papers contrary to policy. And I wonder, Mr. Wells, whether you have any thoughts on that?

Mr. WELLS. Whether it be the survey program, whether it be reducing the minimum requirements that we have testified here today about, given the problems that seem to surface weekly or monthly regarding security lapses, one just clearly comes to the conclusion it is unclear what objective they are trying to achieve when they put forth reductions in surveys and reductions in oversight and reductions in accountability controls.

Mr. COX. Now this same Department of Energy office in Albuquerque comes in for criticism in the Redmond Report for its frustration of counterintelligence programs. Specifically, I am reading now from the Redmond Report: "The Department of Energy Operational Field offices at Albuquerque and Oakland continue to refuse to share relevant information from employee personnel files under their control with the Department of Energy counterintelligence or the lab counterintelligence components. The team," that is, the Redmond team, "learned that Department of Energy counterintelligence is not even informed by these three offices"—by DOE offices with the records, with the files—"when an employee loses his or her security clearance." So counterintelligence can't even find out, because DOE husbands the information and refuses to share it with counterintelligence when an employee loses a security clearance for cause.

Mr. Podonsky, what can we do about this?

Mr. PODONSKY. Well, the first thing I would suggest is that I would—I would want to know whether Ed Curran, the director of the Counterintelligence Office, is familiar with this and if he was, then I would expect Ed Curran and his oversight program of coun-

terintelligence to remedy this in consultation with the rest of the Department that has responsibility over those areas.

Mr. COX. Are you comfortable with the compartmentalization of CI from security?

Mr. PODONSKY. This is an initiative that the Secretary created, and the answer is so far we have been working very closely with Ed Curran's organization, counterintelligence, as well as with General Habiger's security organization. So the answer is we have no reason not to be comfortable with it.

Mr. COX. Do you know what the views of lab management are? We will have a chance to ask them directly in the next panel, but do you know what the lab's view is on this?

Mr. PODONSKY. Other than not necessarily liking Podonsky's oversight organization, no, sir, I don't know what their views are.

Mr. COX. I ask the question because, for example, with respect to human reliability, it is awfully difficult to separate out the expertise that is required for CI from the expertise that's required for security.

Let me read just another passage from this report, the Redmond Report: "It has been the sad experience in many espionage cases that only after the spy is uncovered does it become clear that a plethora of counterintelligence indicators concerning various facets of the individual's life, performance, and behavior have been known in different places by different individuals but never effectively collated or holistically evaluated. The Department of Energy must ensure that the CI officers at the laboratories are part of a formal system set up locally to ensure that all relevant CI and security data information is collected, assembled, and analyzed by means that are not solely dependent on personal relationships"—and on and on.

It is often difficult, it would seem to me, to arbitrarily characterize a bit of information as security information but not CI, or as counterintelligence information but not security. If you have an unreliable person in the building, that's a security issue; it is also a CI issue, isn't it?

Mr. PODONSKY. Yes, sir, and I think that you will find that both the Office of Security Operations and the Counterintelligence work hand in glove, as we also try to ascertain how they are proceeding in some of their operations.

In years gone by, Congressman, the counterintelligence, the intelligence and the security organizations were all contained in the Defense Programs Office and they worked the same way. The difference now is that they all have separate direct reports to the Secretary. So that we have Secretarial attention on these matters.

Mr. COX. I would conclude by observing that Congress created the NNSA, the National Nuclear Security Administration, with a view to centralizing authority over all of these concerns, so there would be a single chain of command, a single line of direction. And we first faced the two-hatting exercise where the Secretary of Energy and the White House decided that they were going to frustrate the intent of Congress and not let the NNSA do its job. We also had a long political delay in getting it started, and only when there was this latest public embarrassment with the hard drives could we even confirm General Gordon as the first Administrator. So

now, a year after passing the legislation, we have it in place but we have all of these efforts to keep power, bureaucratic power and turf in DOE and not let NNSA be the independent agency that it must be to do its job.

I hope that with the experience under our belt, with all of the months and years that are being consumed with people saying that they are doing their jobs but not actually accomplishing it, we can finally see the value of doing this properly, having the NNSA and General Gordon be in charge.

There is one other aspect of the Redmond Report that I think deserves mentioning, and it is the disconnection that this report finds between DOE's glowing reports on its own accomplishments of the initiatives that it has put in place and so on and what actually has been done. What this report says is that whenever an initiative is started or if an order is promulgated, then DOE takes credit for doing it; whereas most of this is unfinished business.

It is a useful remark for the report, and I just wonder whether, Mr. Wells or Mr. Fenzel, you have any comment on that point?

Mr. WELLS. We would agree—and I think we used almost those exact same words earlier in response to a question—that our 20 years' and 50 recommendations' worth of effort in oversight clearly pointed out that they are quick to take action for corrective action, but the implementation isn't necessarily always completed nor is success fully achieved, and the next thing we know the problem recurs.

Mr. COX. Well, Mr. Chairman, I thank you for your indulgence. Mr. Podonsky, I thank you for your efforts in this area; Mr. Wells and Mr. Fenzel as well. It is vitally important that we not make this a fingerpointing exercise and that we get on with it, but there are big changes that have to be made if we are going to get on with it.

While no one means to be critical or fingerpoint, if you have months and months and years and years of inactivity or inadequate response to these challenges, then call it what you will, somebody has to raise hell about it.

Mr. UPTON. Thank you. I think that that leads us to the conclusion of Panel I.

Thank you very much for being with us this morning. You are now formally excused. Thank you. Thank you for your time and your reports.

We will now go to Panel II, that includes the Honorable T. J. Glauthier, Deputy Secretary from the Department of Energy; who is accompanied by General Eugene Habiger, the Director of the Office of Security and Emergency Operations; General John McBroom, Director of the Office of Emergency Operations, and also accompanied by General Tom Gioconda, Deputy Administrator for Defense Programs at the National Nuclear Security Administration; also Dr. Paul Robinson, President and Laboratory Director of Sandia; Dr. John Browne, Director of Los Alamos; and Dr. Bruce Tarter, Director of Lawrence Livermore National Lab; as well as Mr. Steven Aftergood, Senior Research Analyst from the Federation of American Scientists.

It will just take a moment to get the names placed correctly.

As you all know, we have a longstanding tradition of taking testimony under oath. Do any of you gentlemen have objection to that? If not, you are also, under committee rules, allowed to be represented by counsel. Any objection to that? Do any of you desire counsel?

[Witnesses sworn.]

Mr. UPTON. Thank you very much. You are now under oath, and we will start with Mr. Glauthier.

TESTIMONY OF HON. T.J. GLAUTHIER, DEPUTY SECRETARY; ACCOMPANIED BY: GENERAL EUGENE E. HABIGER, DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS; GENERAL JOHN McBROOM, DIRECTOR, OFFICE OF EMERGENCY OPERATIONS; AND BRIGADIER GENERAL TOM GIOCONDA, ACTING DEPUTY ADMINISTRATOR FOR DEFENSE PROGRAMS, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY; C. PAUL ROBINSON, PRESIDENT AND LABORATORIES DIRECTOR, SANDIA NATIONAL LABORATORIES; JOHN C. BROWNE, DIRECTOR, LOS ALAMOS NATIONAL LABORATORY; C. BRUCE TARTER, DIRECTOR, LAWRENCE LIVERMORE NATIONAL LABORATORY; AND STEVEN AFTERGOOD, SENIOR RESEARCH ANALYST, FEDERATION OF AMERICAN SCIENTISTS

Mr. GLAUTHIER. Thank you, Mr. Chairman. Thank you for this opportunity to appear today to provide an update on the security situation at the Department of Energy's weapons laboratories.

I will be brief. My overall testimony has been submitted in writing. I would like to reiterate Secretary Richardson's statement in reference to the missing Los Alamos hard drives. That is, that the Energy Department security procedures were not followed, and since coming to the Department the Secretary has emphasized security issues. We are outraged at what has taken place in this particular incident.

Now, as much as can be discussed, I would like to give a brief update on the current FBI criminal investigation. A grand jury has been convened to examine issues related to the case. It has been determined by the FBI that these are the authentic disk drives. Based upon the investigation by the FBI, there is no evidence of espionage. It can be assured that personnel will be held accountable and disciplinary action will result from this incident, but the Department will not take action until all the facts are established.

During the last 2 years that Bill Richardson has been Secretary, security has been a top priority and the security—and the Secretary has gone to extreme lengths to improve the agency security and counterintelligence profile. Through his leadership, we have implemented over 50 major security and counterintelligence initiatives.

For example, the Secretary has established the Office of Independent Oversight which is headed by Mr. Podonsky that you just heard from, and he is reporting directly to the Secretary. The purpose of that office is to focus on implementation and to give an independent oversight on the practices that are actually being carried out at our various sites.

A lot has been made in the last 2 hours about changes that have occurred in the practices at the facilities. I am sure we will talk more about that. I would comment that the changes that were made over the last decade were changes to introduce more flexibility into the individual practices, the actions that are taken. There was no change in that timeframe on the responsibility for protecting secure information, and I think that is important to recognize that all the individuals at our facilities, all the contractors, all the Federal employees, maintained the same responsibility for protecting secure information throughout this whole timeframe.

And the over 120,000 Federal and contractor employees of the Department of Energy have an outstanding record. Unfortunately, it only takes a few individuals to cause a serious problem which is, of course, what we have seen.

We have implemented additional security procedures in light of the recent incident at Los Alamos, and I would like to just mention a couple of those; things that in some cases changed the kinds of items you were talking about on the earlier chart, and in other cases are new and additional actions, such as encrypting selected classified electronic media, enhancing verification procedures, including log-in and log-out requirements for vault and vault-type room access; staffing all open vaults and vault-type rooms; increasing security measures for certain classified encyclopedic data bases; conducting immediate inventory of all Nuclear Emergency Search Team, or NEST, data; and placing serial numbers and identification codes on sensitive materials.

Additionally, as you probably noticed, the Secretary has informed the University of California that its contract for managing the Department's national weapons laboratories must be restructured in order to bring in a separate organization to be responsible for security procedures and some other facility operations.

Under Secretary John Gordon will oversee the negotiations and work with the university to identify new mechanisms and procedures to address the serious security shortcomings. It is expected that he will have his recommendations to the Secretary by September 5.

The last action that I want to highlight is the assignment that former Senator Howard Baker and former Congressman Lee Hamilton have accepted. Jointly they will conduct a thorough investigation and assessment into the circumstances surrounding the incident at Los Alamos. Their expected assessment, separate from the FBI investigation, will provide recommendations for necessary corrective actions.

In summary, the Department of Energy has a significant responsibility for the American people regarding our overall nuclear security. We are responsible for sustaining America's nuclear deterrent, the cornerstone of our national defense, and for securing nuclear weapons materials and know-how at home and abroad. We must ensure our security measures are stringent, but also that they do not stifle the science that allows us to have that deterrent and that underpins our national security decades into the future.

I know I can speak for my colleagues at the labs and throughout the Department in reiterating our commitment to carrying out this mission in a safe, secure and sensitive manner.

I think General Habiger would like to make a couple of comments, and then Dr. Browne, the director of Los Alamos, in particular wants to comment on these.

[The prepared statement of Hon. T.J. Glauthier follows:]

PREPARED STATEMENT OF HON. T.J. GLAUTHIER, DEPUTY SECRETARY OF ENERGY

Thank you for this opportunity to appear before you today to provide an update on security at the Department of Energy's weapon laboratories.

To begin, at the end of June the Secretary Bill Richardson informed the University of California (UC) that its contract for managing the department's national weapons laboratories must be restructured in order to make much-needed improvements to security and other facility operations. We have begun negotiations with the University to bring into their operations specific security and management expertise to implement these improvements.

Although the Secretary recognizes UC's unparalleled scientific reputation and its contribution to the scientific vitality of the laboratories, he is sharply critical of their failure to bring the same degree of expertise to the management of security and facility operations.

Secretary Richardson has asked Under Secretary John Gordon to oversee this and to work with the University to identify new mechanisms and procedures to address the serious security shortcomings of the University of California at the weapons laboratories. It is expected that General Gordon will make his recommendations to the Secretary by September 5.

SITUATION UPDATE

I would like to reiterate Secretary Richardson's statement in reference to the missing Los Alamos hard-drives, that the Energy Department security procedures were not followed. Since coming to the Department, the Secretary has emphasized security issues. We are outraged at what has taken place. There are no excuses.

Now, as much as can be discussed, I would like to give a brief update on the current FBI criminal investigation. A grand jury has been convened to examine issues related to the case.

The FBI is still looking at the two hard drives found on June 16 at the Los Alamos National Lab. The Secretary has been speaking with FBI Director Louis Freeh throughout the investigation.

It has been determined by the FBI that these are the authentic disk drives. Based upon the investigation by the FBI, there is no evidence of espionage.

The Bureau continues to treat the area where the hard drives were found as a crime scene. Over the last several weeks, the FBI and Energy Department investigation has focused on a handful of X-Division employees, who have offered conflicting statements to investigators.

I can also tell you that, according to its latest findings, the FBI's working theory puts the loss of the drives at the tail end of March of this year. This time-line would be further refined as the investigation continues. This information helps clarify some details surrounding this case.

Prior to this incident, the Secretary's directive required the Department to be notified of any such problem within eight hours of their discovery. That is his policy. Instead, the University of California neglected to inform the Department until three weeks after the initial discovery.

As you know, the Department immediately brought in the FBI, informed the President, advised others in the Administration with a need to know, and shared what we knew with the relevant Congressional committees.

It can be assured that personnel will be held accountable and disciplinary action will result from this incident. But the Department will not take action until all the facts are established.

LATEST SECURITY ACTIONS

During the last two years, security has been a top priority, and the Secretary has gone to extreme lengths to improve this agency's security and counterintelligence profile. Through his leadership we have implemented more than 21 major security initiatives and have completed 36 recommendations in the Counterintelligence Implementation Plan.

However, when the recent breach came to our attention, we immediately implemented an elevated slate of security procedures to be followed in our sensitive divisions. I reviewed a number of enhanced security protection measures directed by

General Eugene Habiger, Director of Security and Emergency Operations, and who is with me. These new steps will effect immediately. They include:

- Encrypting selected classified electronic media;
- Enhancing verification procedures for vault and vault-type room access;
- Manning all open vaults and vault-type rooms;
- Evaluating existing vault and vault-type room procedures;
- Increasing security measures for certain classified encyclopedic databases; and,
- Conducting an immediate inventory of all Nuclear Emergency Search Team (NEST) and Accident Response Group (ARG) assets.

These steps are in addition to measures the lab has put in place:

- Placing serial numbers/identification on sensitive materials;
- Changing combinations to vaults; and
- Reviewing vault access policy, including a vault "stand-down" to ensure procedures are followed.

NEST

Next I would like to give a description of the Department's Nuclear Emergency Search Team, familiarly known as NEST, and the policies and procedures in which it operates.

NEST is one of seven major Department of Energy Emergency Response assets tasked with responding to nuclear incidents or accidents. NEST members are dedicated volunteers who, when called, form a highly skilled force specially trained to deal with all types of nuclear and radiological emergencies.

The concept of the response teams and how the program runs on a daily basis may provide some valuable insight. Ordinarily, the Department has no standing teams formed. The all-volunteer personnel who would comprise these teams are working their normal jobs within the lab/site structure. An example of this concept would be a volunteer fire department in which a member's full time occupation is working in the local school system. That person only becomes a responder when the siren goes off; up until then he or she is a school teacher.

Similarly at the Department, when an event such as a training exercise, or an actual emergency occurs, the Secretary, through the Director of Security and Emergency Operations "stands-up" a response team. Until that time, most personnel are working full time on the laboratories' scientific and technical missions.

Once a team is formed, the operational responsibility shifts from the laboratory to the Department's headquarters chain of command. The administrative responsibility continues with the laboratories. For example, the Director of Emergency Management cannot fire or suspend a University of California team member, however, the ultimate administrative responsibility continues with the laboratory's director.

Training deployments or real world events, such as the World Trade Organization meeting in Seattle,Washington or the 50th NATO Summit in Washington, DC, present unique and difficult challenges in moving and securing the classified equipment on the road. Sometimes the teams work in US cities and other times they find themselves in overseas locations.

RECENT REPORTS

Now I would like to take this opportunity to address recent reports criticizing the Department's security.

We have recently reviewed the Inspector General's report entitled "Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory." We are concerned about these results, particularly with respect to the reported changes to the 1998 and 1999 surveys without providing a documented rationale for the changes. We note however, that making such ratings decisions always involves a degree of objective judgment.

However, we are more concerned with the reported destruction of work papers regarding the survey ratings at the Albuquerque Operations Office, and reports that thirty percent of the laboratory security staff felt pressured to "mitigate" security self-assessments and other related allegations. We are reviewing the report carefully and are not ruling out changes to existing procedures regarding our security surveys and self-assessments. We also are reviewing the role and actions of the personnel involved in these particular surveys and assessments, and stand ready to hold personnel fully accountable for any improper actions taken, if our review indicates that to be the case.

I will now discuss the responsibilities of the Department's Counterintelligence (CI) Program inspections. This program was directed by Presidential Decision Directive No. 61, which directed the establishment of a CI Program at Energy, and the in-

spections of the CI Programs in the laboratories, sites and operations offices. These inspections assess program performance in seven topical areas, which include subjects such as investigations, training, analysis and management. The inspections also evaluate the degree to which the programs are in compliance with the measures identified by the CI Implementation Plan.

The CI Programs of the three national laboratories were inspected in August, September and October of 1999. As the Committee knows, the CI Program at Lawrence Livermore received a satisfactory rating. The CI Programs at Los Alamos and Sandia, however, received a marginal and an unsatisfactory rating, respectively. Many of the problems stemmed from the newness of these CI Programs and the personnel involved. Shortfalls identified by the inspections were responded to in corrective action plans developed by the programs; progress on the corrective actions was tracked by Office of Counterintelligence management.

The Office of Counterintelligence reinspected the Los Alamos and Sandia CI Programs in April of this year. These special inspections focused on the problem areas that were identified during the initial Inspections. In both cases, the inspections found that the corrective actions had been completed and both programs received satisfactory ratings. The Lawrence Livermore CI Program will be reinspected in September.

Next, I would like to make a few comments on the recently publicized General Accounting Office (GAO) report on the Department's foreign travelers. The Department agrees with the GAO that travelers to nonsensitive countries may also encounter incidents similar to those experienced by sensitive country travelers and that any Department employee traveling overseas could be an intelligence target. It is true that the initial focus of the CI Program has been on Departmental employees working in classified programs who have sensitive country contact. However, our CI Program does not focus only on those employees and programs. The Department's Counterintelligence Program collects information of any kind or any location that may show a foreign intelligence presence. Moreover, all employees and contractors are required to receive an annual CI awareness briefing that instructs on the methods and capabilities of foreign intelligence services. During these briefings, employees are instructed to inform their CI officers of anything they observe that may be an indicator of intelligence activity.

In short, our relatively new CI Program, which truly only got underway after Secretary Richardson arrived to the Department in late 1998, leaves the Department far better prepared to protect its personnel and programs overseas than ever before. Our defensive CI Program now can be said to be one of the best in government, and it will continue to improve. The fact that the report cites a number of overseas incidents is not an indicator of CI Program deficiencies; rather, the existence of these incident reports demonstrates that Energy's CI Program is getting the information it needs to build a good defense to these ongoing hostile intelligence activities. Moreover, as a result of the incident reporting the CI Program is getting, we believe we are steadily improving our ability to get the message to our employees on how they can protect themselves during overseas travel.

LARGER PICTURE

The Department of Energy has a greater charge from the American people. Our overall nuclear security. It is a task far more complex than can be described by me or debated to a satisfying conclusion here today.

We are responsible for:

- Sustaining America's nuclear deterrent—the cornerstone of our national defense; and
- Securing nuclear weapons materials and know-how—at home and abroad.

The Department has taken its security responsibility very seriously. The challenges of the Department of Energy have crossed decades and administrations.

Ultimately, security will always also be an individual responsibility, and must rely on the dedication, loyalty, and patriotism of our weapons scientists. And these people must be accountable like anybody else. Individuals are, indeed, fallible, and no amount of policy—no amount of legislation—will protect us from irresponsibility and human failings.

We must remember that a successful security policy is one that results in the detection of security violations. The worst security violations are the ones that go undetected. We will continue to keep you and other key Congressional committees informed of further developments immediately as they become available.

Thank you for this opportunity to appear before you today to provide an update on security at the Department of Energy's weapon laboratories.

Mr. UPTON. General Habiger.

Mr. HABIGER. Mr. Chairman, thank you. I just want to clarify three things. First, I am a little disappointed at our colleagues from the General Accounting Office in terms of the chart that they put up there, in terms of what you saw was characterized as Department of Energy. What you saw in that chart is across the government in every respect. That's point No. 1.

Point No. 2, and I think it is equally important, is if you—if he had included time lines, you would have clearly seen that we didn't get credit for dragging our feet like we normally do. We lagged the rest of government for some very, very good reasons.

Point No. 3, sir, Ms. DeGette raised the point about human reliability program and a letter from Podonsky to Habiger.

Mr. Chairman, I asked for Glenn's input because I had only been in the job 6 weeks and I saw we had two human reliability programs at the Department of Energy. It didn't make sense; two different rice bowls. It has taken awhile, but we are in the final stages of putting out a strengthened single human reliability program.

But to characterize questions to Glenn as to whether or not I accepted his inputs, I am the one that asked for those inputs. Thank you, sir.

Mr. UPTON. Thank you.

Dr. Robinson.

TESTIMONY OF C. PAUL ROBINSON

Mr. ROBINSON. Thank you very much, Mr. Chairman. It is a pleasure to again be with you. I did prepare a formal written statement for the record, and with your permission——

Mr. UPTON. All the statements will be made a part of the record.

Mr. ROBINSON. Good. I will summarize and move to your questions.

Several of you, in fact, visited our laboratories to sample the security environment. You saw for yourselves the physical security measures, the personnel security measures both to enter or egress from one of our facilities. We discussed the challenges which cyber security is placing before us and some of the measures we are taking to counter that threat.

Most of you know the unique missions of Sandia National Laboratories: U.S. nuclear weapons, related areas of nuclear intelligence and nonproliferation. You may not be aware of our mission responsibilities in security research and development, both for nuclear weapons storage and transport, and computer security technologies. We carry these functions out for not only the Department of Energy but for other high-security agencies as well.

Because of these core responsibilities, we believe we should and can be held to a higher standard for security, and I believe the record will show that we are meeting that higher standard.

Now, this is certainly not an area to ever be boastful. Security is something that does require eternal vigilance. I will try to explain, and I think I try to discuss in my testimony, the complexity that accompanies security. Most importantly, at its heart, security requires the care and devoted effort of the people who perform the

classified work. There is always the danger of a mental lapse, a mental lapse which could cause great harm.

Besides trying to design in approaches of defense and depth into all of our security practices and procedures, which could allow for that inevitable human error that will occur, we must also involve our people, those who carry out the classified work in the design of the best practices. I believe their understanding, their faithfulness, their care in fulfilling these duties as holders of our important secrets is an essential part of the formula for success.

In my testimony, I would like—I do describe security management at Sandia; our unique role within emergency response functions, our controls to protect classified material, both documents and electronic media. We have made more stringent controls on vaults and vault-like rooms.

Finally, in that wonderful clarity that's hindsight, I do discuss some of the weaknesses, both in document accountability and in classification, or rather declassification. I think these are areas where we can all agree we need to make improvements.

Let me close with the statement that I said in my formal text. I have been in classified work, associated with nuclear weapons, for just over 32 years. I can validate Secretary Richardson's remark several weeks ago that indeed he has done more to focus on and improve security than any prior Secretary. Doubtless, that is true, but I believe we are all culpable. Indeed, across the government, standards were lowered after the end of the cold war, in classification and accountability for classified documents and levels of background investigation to obtain clearance to work at our laboratories.

Also, we have been facing in more recent years a growing threat of cyber security which is real and it is challenging.

What is the road back? I think we need to use the opportunity you have provided us in the creation of the NNSA to streamline responsibilities and accountabilities, to clear out the bureaucracy that often confuses this line and paralyzes actions by both Department Secretaries as well as laboratory directors. I want to assure you, we did not lose our concern for security. We are a unique enterprise, conducted on behalf of the Nation. We can and we will strengthen the protections to once again win your respect to manage nuclear weapon affairs with confidence. Thank you very much.

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

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

INTRODUCTION

Mr. Chairman and distinguished members of the committee, thank you for the opportunity to testify today. I am Paul Robinson, director of Sandia National Laboratories. Sandia National Laboratories is managed and operated for the U.S. Department of Energy by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation.

Sandia National Laboratories is a multiprogram laboratory of the National Nuclear Security Administration (NNSA). We share responsibility for the design and stewardship of nuclear weapons with Los Alamos and Lawrence Livermore National Laboratories. Sandia's job is the design, development, and certification of nearly all of the non-nuclear subsystems of nuclear weapons. Our responsibilities include arming, fuzing, and firing systems; safety, security, and use-control systems; engineering support for production and dismantlement of nuclear weapons; and surveillance

and support of weapons in stockpile. We perform substantial work in programs closely related to nuclear weapons, such as nuclear intelligence, nonproliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also performs research and development for DOE's energy offices, as well as work for other agencies when our unique capabilities can make significant contributions.

SECURITY AND BUREAUCRACY

I appreciate your invitation to make a statement today addressing the topic, "Weaknesses in Classified Information Security Controls at DOE's Nuclear Weapon Laboratories." Secretary Richardson said in testimony before the Senate Armed Services Committee on June 21 that he has done more to improve security during his two years in office than had been accomplished in the previous twenty years by his predecessors. I have been active in the DOE/AEC community for all my career, and I can vouch for his claim. Yet, for all the well-motivated actions and strong leadership that has been so evident, I cannot say that our important restricted data and national security information are more secure than ever before. My hesitancy derives from a surfeit of complications that surround security.

The Secretary and the laboratory directors share the same desire for effective security performance; we are not at odds. But I believe we are both stymied by the bureaucratic sclerosis of the agency. From below, the laboratories are frustrated with a maze of conflicting rules and directives from various offices of the Department, together with team after team of inspectors that descend upon us. From above, the Secretary has resorted to managing the security problems by issuing directives from his own office, rather than relying on the agency's internal mechanisms to generate and implement reforms. This game of catch-up between the top of the agency and those who must implement the directives, with far too little communication on the chances for success or the unforeseen consequences of new policies, has been a problem in almost all areas of support for DOE missions—in environment, safety, and health issues, in business practices, and in security.

The President's Foreign Intelligence Advisory Board (PFIAB) appreciated the magnitude of this problem. Their report, "Science at Its Best; Security at Its Worst," issued last year, referred to DOE as a "big, byzantine, and bewildering bureaucracy." In regard to security performance, the PFIAB found that "multiple chains of command and standards of performance negated accountability, resulting in pervasive inefficiency, confusion, and mistrust" (page I). It concluded that "real and lasting security and counterintelligence reform at the weapons labs is simply unworkable within DOE's current structure and culture" (page 46). The PFIAB's recommendations, of course, were the impetus for the legislation creating the semi-autonomous National Nuclear Security Administration within the Department of Energy.

It is my belief that the circumstances in DOE are not the fault of any individuals, certainly not the people who are in charge or occupy key positions in the Department of Energy today. As the President's Foreign Intelligence Advisory Board found, the single most identifiable factor that led to the current state of affairs was the relentless growth of bureaucracy. My definition of bureaucracy is when well-meaning, capable people find it difficult to accomplish their mission responsibilities because of multiple lines of authority and bureaucratic hurdles that must be overcome.

I believe the National Nuclear Security Administration is our last best hope for fixing our security problems in a systematic way. By "fixing" I mean creating a security culture across the complex (federal workers and contractors) that achieves teamwork and mutual commitment to the goals of security. As things stand now, there is little sense of collaborative work toward a shared goal in security. Security in DOE is a "house divided"—those who make the rules, and those who must follow them. There is little discussion with the field by those who write guidance and policy. The people who really know the technologies that can be helpful have little input. It is, as has been said before, a "dysfunctional" relationship.

The new administrator of the NNSA, General John A. Gordon, has quite a challenge before him. But as qualified and as competent as he is, he will not succeed unless he has full authority and free rein to redesign the structure of the nuclear complex from the ground up. I know that the laboratory directors and the federal managers of the NNSA will fully support him in this undertaking.

SANDIA HAS A POSITIVE SECURITY CULTURE

An erroneous perception has arisen that the laboratories have a culture of indifference or even contempt for security. I can tell you that this perception is grossly inaccurate for Sandia National Laboratories, and I believe it is inaccurate for the other NNSA laboratories as well. Certainly we have had challenges and problems

in various aspects of security performance, but I take issue with the belief that we have an ingrained or widespread "attitude problem" toward security at Sandia.

Sandia's laboratory culture was shaped by its industrial heritage, which began in 1949 under the management of AT&T Bell Laboratories and continued after 1993 with Lockheed Martin Corporation. Our industrial roots gave us a strong cultural commitment to security. Industrial laboratories are very conscious of the need to keep proprietary information secure. As I enumerated in previous testimony to this committee, Sandia has a long history of originating and implementing innovations that have improved security without direction from DOE (see Questions for the Record for my testimony to this subcommittee on October 26, 1999). And we also have a history—as I will illustrate later in my statement—of challenging policy changes mandated from above that would weaken our protections and controls on classified materials.

In June 1999, the Secretary of Energy called for a stand-down of operations at the Defense Programs laboratories to conduct an intensive two-day session of security training. Contrary to reports that laboratory staff were resistant to this training, our staff participated with great interest and with a positive attitude. We had 93 percent staff participation during the stand-down, and we achieved the full 100 percent shortly thereafter. (The seven percent difference consisted of people on previously scheduled vacations or essential business travel, illness absences, and critical job functions such as security and medical staffing.) The thoughtful dialog and suggestions offered by employees during the security sessions clearly demonstrated a laboratory culture of positive concern and advocacy for effective security.

I was not at all surprised that the inspectors from the DOE Office of Independent Oversight and Performance Assurance remarked on the positive and cooperative attitude among Sandia managers with whom they worked during the 1999 inspection of Sandia National Laboratories. I frequently get similar comments from other audit and inspection teams. Sandia has a culture of respect for security, and people notice it. At the close-out meeting of the most recent visit of the DOE Oversight and Performance Assurance Team in June, it was encouraging to receive informal verbal feedback from the inspectors to the effect that Sandia is currently meeting all requirements and is above and beyond minimal requirements in many areas. The team commented that they found it refreshing to see a sense of ownership for security at the manager level. They also remarked that Sandia's custodians of classified matter are well-versed in their responsibilities; they know what to do and are doing it well.

SECURITY MANAGEMENT AT SANDIA

Sandia has implemented an Integrated Safeguards and Security Management System (ISSMS) for all its security responsibilities. As the name implies, the goal of Integrated Safeguards and Security Management is to incorporate responsibility for security into the daily work of every employee. We can't just bring in security experts and give them the job of inspecting-out the defects; every single person bears responsibility to build-in and maintain sound security measures. This is a necessary attribute of a stable security culture.

ISSMS establishes clear and unambiguous lines of authority and responsibility for ensuring that secure operations are established and maintained at all organizational levels. Authority and responsibility for security at Sandia National Laboratories begins with me and flows via my deputy laboratory director to the line vice presidents that report to her. Sandia's Chief Security Officer coordinates the enabling resources that support the line executives in their security responsibilities. ISSMS ensures that personnel possess the training, knowledge, and abilities necessary to discharge their security responsibilities. It also provides a way to allocate resources efficiently to address security and operational needs.

Our ISSMS methodology stresses the need to identify applicable security standards and requirements before work is performed. Administrative and engineering controls to prevent and mitigate security risks are tailored to the work being performed and are designed into work processes. While we make use of a "fresh-set-of-eyes" in examining security practices and draw on the knowledge and experience of security professionals, we gain the involvement and creativity of those actually carrying out the work in developing security procedures that make sense in the workplace.

SANDIA'S PARTICIPATION WITH THE NNSA'S NUCLEAR EMERGENCY SEARCH TEAM (NEST)

The National Nuclear Security Administration plays a vitally important support role in combating acts of nuclear terrorism through its Nuclear Emergency Search Team (NEST). NEST provides the FBI with technical assistance in response to ter-

rorist use or threat of use of a nuclear or radiological device in the United States. NEST also supports the State Department in a similar role overseas. Another team, the Accident Response Group (ARG), has the different mission of providing technical support in response to accidents involving U.S. nuclear weapons while they are either in the custody of DOE or the military services.

The highly selective force that makes up the cadre of deployment personnel for NEST and ARG are mostly from the nuclear weapons laboratories. To be on the NEST team, an individual must be approved by both line and program management, have certain essential technical skills, pass a physical examination, and take additional training. My experience is that NEST members are conscientious and dedicated individuals with a high sense of duty. NEST personnel volunteer for a mission which, if not successful, could have severe consequences for the nation and be fatal for the team.

Sandia National Laboratories contributes a number of team members to the NEST. Sandia does not possess any NEST computer media similar to that reported as missing by the Los Alamos group. Sandia's role in NEST is different from that of Los Alamos and Lawrence Livermore, focusing largely on the non-nuclear electronic subsystems of warheads and bombs as well as methods for calculating the consequences of dispersal events and methods for containment.

Sandia does maintain some classified computer media and lap-tops under the ARG program. This information is significantly different from the NEST media at Los Alamos. This classified material has all been accounted for. Furthermore, within the last three weeks, we instituted stricter controls for these items, including a two-person rule and formal sign-in/sign-out procedures.

CLASSIFIED MATERIAL PROTECTION AND CONTROL

Sandia employees and contractors who handle classified matter are required to protect and control classified material from unauthorized, casual, and deliberate access. This requirement is one of the first things a new-hire is briefed on when he or she joins Sandia National Laboratories, and we continue to educate our personnel on the procedures that implement this policy throughout their careers through annual refresher training courses.

The core principles that we teach our employees regarding access to classified material are contained in Sandia's Safeguards and Security Guide, which is readily available as a reference on our internal network. Access to classified matter requires a job-related need-to-know, as determined by an individual's manager, as well as a proper security clearance.

As you know, Secretary Richardson distributed a memorandum on June 19, 2000, directing the implementation of certain enhanced protection measures at the NNSA laboratories. I welcome the emphasis on accountability that the memorandum so clearly communicates. Sandia took immediate steps to implement or commence work on the enhancement measures that are the responsibility of the laboratories, and we will cooperate with the NNSA offices responsible for implementing other measures in their purview.

Controls for Vault Access

Sandia has explicit rules governing the storage of classified matter. Briefly, classified material must be stored in vaults or vault-type rooms (or in a military-style igloo similar to a vault-type room), or in key- or combination-lock containers approved by the General Services Administration and located in a locked and alarmed building. Sandia National Laboratories manages 166 vaults or vault-type rooms that store classified matter (documents or material)—114 at our New Mexico location and 52 at our California site.

In compliance with Secretary Richardson's memorandum of June 19, 2000 (received late on June 20), Sandia modified operating procedures for all vault access on June 21. We modified our log sheets to record the entrance and exit of all personnel. We also required that access/egress points for vaults be under continuous, positive control by personnel authorized for access to that specific vault. Or, for vault-type rooms (large vaults in which a number of people work) we required that the vault be occupied and that access by authorized personnel be controlled by an electronic system. In the absence of these controls, the vault must be in a locked and alarmed state.

Controls over Electronic Media

On June 15, 2000, Sandia's chief information officer initiated a lab-wide survey of removable classified electronic storage media. The objective of this survey was to determine that removable media are accounted for (to the extent possible in the absence of formal document accountability) and are properly stored. The survey found

that all holdings were accounted for, except for two relatively minor issues which were immediately communicated to DOE via the Department's incident reporting system. The first issue involved a set of unclassified commercial software program disks that were treated as classified. The inquiry is still active, but has concluded that those disks contained no classified information. The other issue (reported on June 30) involves a single 3½ inch, 1.44-megabyte diskette that has not yet been located. An inquiry is currently underway in accordance with DOE procedures.

Significant overall improvements in the cyber-security of the nuclear weapons complex have been accomplished at substantial cost in 1999 and 2000. However, many potential vulnerabilities continue to present formidable challenges to computer security. There are no easy solutions. Although encrypted removable media or media-less computing may have their places in a defensive system (and I believe they do), there are many ways for a sophisticated adversary to extract information in today's modern electronic environment. Removable media, email, hot mail, ftp file transfer, http file transfer, port-enabled file transfers, laptops, modems, network sniffers, video-monitor-to-VCR converters, faxes, mail, copiers, two-way pagers, telephones, cell-phones, and computer trash are all potentially exploitable. Cyber-security is certainly the most formidable security challenge facing DOE and the federal government as a whole.

Because of the magnitude of the cyber-security challenge, a systems approach across the entire NNSA complex is required. I am very pleased that emergency supplemental funding for cyber-security upgrades has been approved by Congress as part of the FY2001 Military Construction Appropriations Bill. The funding is badly needed to combat cyber threats and vulnerabilities in a coordinated fashion throughout the nuclear weapons complex.

WEAKNESSES IN THE DOCUMENT ACCOUNTABILITY PROGRAM

Prior to 1991, DOE practiced full document accountability for all Secret data under its control. Document accountability was a formal system for inventorying and recording access to classified documents over the lifetime of the document, from creation to destruction. The system was analogous to—although much more rigorous than—the common library check-out system that was aptly cited by a member of this committee.

In February 1991, DOE modified its accountability rules to drop the requirement for formal document accountability over Secret National Security Information and "non-weapon Secret Restricted Data." (Restricted Data is a category of protected information created by the Atomic Energy Act that includes "data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power.")

In May 1992, DOE extended its Modified Accountability Program to include weapon-related Secret Restricted Data. DOE notified the laboratories that accountability requirements were being modified for all categories of Secret data for organizations that had met certain requirements, including having completed a 100 percent inventory and reconciliation of controlled documents in accordance with DOE Order 5635.1A.

The Modified Accountability Program was instituted by DOE to accommodate the National Industrial Security Program, which was intended to standardize security requirements among all federal agencies. It should be noted that prior to the Modified Accountability Program, DOE protected Secret Restricted Data with the same level of protection employed by the Department of Defense for Top Secret.

The modified accountability program eliminated the requirements for unique document numbers and maintenance of accountability records for documents, inventories, destruction certificates, written authorizations to reproduce, and some internal receipting. Other security procedures not explicitly changed by the modified accountability program were unaffected.

Unfortunately, with the change in accountability, DOE lost the ability to track who was accessing which secret documents, a feature that had been a useful tool for counterintelligence analysis. While this change clearly saved money and made sense in the broader context of consistency across all federal agencies, it reduced our ability to quickly detect the absence of a document, and it eliminated our capability to formally monitor the access to secret classified matter. This statement applies to documents and information in printed form as well as to electronic media.

The laboratory directors were never comfortable with the change to Modified Document Accountability. At Sandia, we originally told DOE that we intended not to implement the Modified Accountability Program. In response, DOE told us that costs for full accountability would no longer be reimbursable under the operating

contract. Sandia complied with DOE's requirement, but we left open local options for higher levels of accountability.

In January 1998, DOE moved to eliminate full document accountability for Top Secret Restricted Data as well (and for other categories of Top Secret information). As part of this change, DOE eliminated the "Top Secret Control Officer" positions at the laboratories. I am proud to say that staff at Sandia had better sense and continued to protect Top Secret data with full document accountability—a decision that I have fully endorsed.

Sandia National Laboratories has consistently maintained full accountability for all Top Secret data under its control. And in fact, we have also maintained document accountability over selected sets of Secret data that we felt merited ongoing accountability. These examples demonstrate the culture of respect for security that exists at our laboratory. Rather than resisting efforts to improve security (as has been charged by some critics of the laboratories), the record shows that we are more likely to resist efforts to weaken it.

On March 1, 1999—following a conference call of the three nuclear weapon laboratory directors with Under Secretary Ernest Moniz on the topic of Secret and Top Secret accountability—I faxed a request on behalf of the directors to the Under Secretary in which we recommended that the former controls over document accountability be reinstated as quickly as possible. We requested that the Under Secretary and the Department's counterintelligence official evaluate the feasibility of promptly reinstating full document accountability. This request was submitted to the Department's security bureaucracy, and to our knowledge it has never emerged.

I have twice brought the modified accountability problem to the attention of Congress in testimony: in my statement to the Senate Committee on Energy and Natural Resources on May 5, 1999, and to this very subcommittee on October 26, 1999.

In my judgment, we can no longer afford to wait for official reinstatement of the full document accountability policy. The security and counterintelligence benefits afforded by formal accountability decisively outweigh the costs. Moreover, formal document accountability will help protect conscientious employees from the indignity of criminal suspicion similar to what some employees had to endure in the recent Los Alamos incident. Therefore, I have decided that Sandia National Laboratories will re-implement formal document accountability for Secret Restricted Data under its control at the earliest feasible date. I have directed Sandia's Chief Security Officer to develop an implementation plan for this change.

WEAKNESSES IN THE CLASSIFICATION PROGRAM

In parallel with the changes in document accountability introduced by the Department of Energy in the middle 1990s, changes were also made to DOE's classification program that, in my view, introduced systemic weaknesses.

A Fundamental Classification Policy Review was recommended by a Classification Policy Study in July 1992. Based on that recommendation, Secretary Hazel O'Leary committed DOE to review all classification policies and related technical guidance, and then to revise classification guidance to reflect changes in policy. DOE's Fundamental Classification Policy Review was initiated in March 1995, and was a major component of Secretary O'Leary's Openness Initiative.

In April 1995, the President issued Executive Order 12958, "Classified National Security Information." This directive modified some of the existing rules concerning classification, but it introduced significant new provisions requiring agencies to perform large-scale reviews of material for potential declassification. However, the order explicitly exempted Restricted Data (RD), which is governed by the classification provisions of the Atomic Energy Act.

Even though Executive Order 12958 excluded Atomic Energy Act Restricted Data, the directive dramatically influenced DOE's thinking toward classification and declassification of RD during its Fundamental Classification Policy Review. The review concluded in July 1996 with recommendations for regulatory changes that substantially applied the provisions of Executive Order 12958 to Atomic Energy Act Restricted Data. The new regulations (10CFR1045) required large-scale periodic and systematic reviews of RD documents for declassification "based on the degree of public and researcher interest and likelihood of declassification upon review."

The declassification regulations, while well-intentioned, required a level of effort by the Department that it was not equipped to handle. As a result, the primary emphasis and deployment of manpower in the classification organization at DOE changed from effective administration of classification responsibilities to effective management of the declassification efforts. The organization even changed its name from "Office of Classification" to "Office of Declassification."

It should be noted that some federal agencies used the process of "bulk declassification" as a mechanism to meet the requirements of Executive Order 12958. This practice often resulted in inappropriate information being released into the public domain without document-by-document review. The negative impact of these actions is still being felt today throughout the federal government.

It has become evident in the last few years that DOE's classification program is in crisis. As a profession, the classification field has become needlessly complex and arcane. The federal government's classification rules evolved over several decades and from different agencies, and they are rife with inconsistencies and legalistic complexities. The system is poorly indexed and coordinated. DOE classification officers rely on a body of some eight hundred sources of classification guidance for DOE source material alone; and they must be familiar with hundreds of other sources that govern the classification of National Security Information from other agencies. Classification professionals in the DOE community—and they are all technical-degreed personnel—often must use their subjective good judgment to resolve conflicting or unclear guidance.

To their credit, the DOE Office of Declassification embarked on a "Guidance Flattening Initiative" two years ago which should go a long way toward simplifying classification guidance and reducing conflicts. It would also be helpful if the classification community could define subsets of need-to-know categories to help us in administering the need-to-know principle. However, the classification community in DOE is disproportionately assigned to the management of the declassification effort, with a need to devote more effort to the efficient and effective management of the classification program.

IMPACT OF SECURITY ON THE WORK ENVIRONMENT

As a laboratory director, I am responsible for maintaining in top condition the infrastructure and human talent of one of the nation's foremost laboratories supporting vitally important national security objectives. I am worried about our pool of human talent to carry out this mission. Clearly, the NNSA laboratories need to continue their focus on enhancing security. But if security enhancements are implemented in a way that creates an atmosphere of mistrust, or generates unnecessary procedural burdens, or is perceived to be discriminatory against some groups, or dictates prescriptions that technical people have no input to, then the talent pool at the laboratories will begin to suffer.

Even without the security issues that the laboratories face today, we would still be having a tough time attracting and retaining talent in an economy that offers very attractive opportunities to technical graduates. Frankly, we are beginning to have a serious multidisciplinary staff retention issue. Poorly thought-out security and human reliability programs will only make that situation worse.

Rather, the NNSA must strive to create conditions that make security a natural way of doing one's job. We need user-friendly work environments that incorporate robust security features in a way that achieves maximum protection for secrets with minimal obstruction of productive activity. I am certain that the best solutions will be system solutions that begin by focusing on specific work activities and move outward from there to establish rules—as opposed to those that begin with rules, directives, and policies that originate at a great distance from the workplace. Robust and lasting security can only be achieved through the cooperative efforts of the laboratories, their M&O contractors, and NNSA management, with the firm but supportive oversight of Congress.

Mr. UPTON. Thank you very much. The second bells are just about ready to ring, so we are now going to adjourn until 1 o'clock, and we will start with Dr. Browne when we come back. Thank you.

[Brief recess.]

Mr. UPTON. Thank you, everyone, for being prompt and coming back.

Dr. Robinson, thank you for your testimony.

Dr. Browne, welcome.

STATEMENT OF JOHN C. BROWNE

Mr. BROWNE. Mr. Chairman, members of the committee, thank you. It has been 6 weeks since I first found out about these missing hard drives. That was on June 1 of this year, and my anger and

frustration has increased over these 6 weeks because we have not been able to understand how this incident occurred or, in fact, what led to even the missing hard drives being found on June 16. Their finding really gives me no comfort, and we certainly did not celebrate. We were pleased that we had control back of the hard drives, but we were not pleased because we did not understand the circumstances.

I would like to clear up something for the record. It has been stated that the University of California did not notify the Department of Energy for over 3 weeks. It is true that some employees at the laboratories kept that information from my management team. But when we found out, we immediately and promptly notified the Department of Energy. As a matter of fact it was less than 2 hours between the time I was informed and the formal notification of the Department of Energy.

I would like to start out by saying that there are no excuses that I can give you for this hard drive incident, and I certainly did not want to come here and point fingers between myself and the Department of Energy. When we look at this, there may be some contributing factors. Again, none of them really are excuses, but they are contributing factors. One is, I do think that we have to look at the adequacy of both DOE laboratory procedures and practices, both to prevent and detect this type of incident. I think we have to determine whether our human reliability programs are adequate. And did we have the appropriate oversight of a closely held need-to-know program like NEST, and fundamentally, did we have the right formality of operations in the NEST program.

Let me say that I am accountable for the actions at Los Alamos National Laboratory, and I take those responsibilities very seriously. We have taken significant corrective actions since the finding of the hard drives being missing, and I will take disciplinary action once the FBI case has been concluded, I have been precluded from further internal investigations by the FBI.

I believe we must return Secret RD and Top Secret to accountability and tracking. There is a cost and a time factor involved. I think we should review our human reliability programs to make sure we have the right people and we have the right program in place.

Science is essential to do our mission. We will fail without science. But it is not sufficient. If we have indifference or carelessness on the part of any of our people, regardless of their scientific or technical accomplishments, we cannot allow that to occur and to affect national security.

I think the challenge facing General Gordon and the NNSA is to reinforce the security culture while maintaining science at its best. And I think he should be given the opportunity to do that, and we certainly will support him in that. Let me make just a few points. We have discussed a lot this morning, the 1990 period of security deemphasis. I will not go into any more of that. I think it has been covered pretty clearly.

I would like to point out that before this committee last year, I think all three laboratories testified to the point that we felt L Clearances and the use of L Clearance as a default clearance was

a mistake and that we would prefer to have Q Clearances at our site. And I think we still feel the same way.

Also the color of badges. We brought that up saying that we thought a single-colored badge really hurt our ability to maintain security environment at our laboratory. The Department has returned to a colored-badge system that we think is very effective now.

When I became director about 2½ years ago, I started a lot of security enhancements. I have increased the budget that we spend on security by 50 percent in the last 3 years. We have made improvements in cyber security, counterintelligence, and since the hard drives incident, we have been logging people in and out of vaults since about June 12. We now have our computer media, the high-density type of media, whether they are hard drives or Zip drives or any of that type, we have 66,000 of those bar-coded, and they are able to be tracked.

We are waiting for guidance from the Department of Energy on how best to put in place a tracking system that is consistent across the entire Department of Energy so that we do not have incompatibilities between various sites.

Let me mention something that Mr. Podonsky brought up this morning, which I think is a very important issue about the role of UC in the laboratory and the Department of Energy. I know my time is up, but if it is okay, I would like to make this point. It is a shared and joint upon responsibility.

There is no doubt that the University of California signed a contract with the Department of Energy, which assigns responsibility for security to the university, and that as an officer of the university, they delegate that responsibility to me as laboratory director.

And I accept that responsibility. The Department shares, I believe, in our accomplishment of that, because they do set rules. They do evaluate our performance, and they also provide the resources. And I think it is important for the committee to realize that there are no separate resources provided for security. The security dollars come out of the programs directly. Which means there always has to be a prioritization between safety, security, programmatic. And it is a balancing act that both the labs and the DOE have to maintain.

With that, I will stop and be happy to answer any questions that you might have. The last statement I guess I would like to conclude with is I would hope this committee does not judge all 8,000 Los Alamos employees by the acts of a few individuals. Our people are really dedicated to national security. I would like to tell you today that they are hurt and angry. They feel let down by their other employees. People are really angry. I get lots of e-mail from laboratory employees who have been pretty outspoken about this latest incident in the wake of the one a year ago. I believe that science and security can coexist. I think it is critical to our Nation's defense, and I believe that we need to move on from this incident; learn from it, but not throw out the good things that we have and are doing for our country. Thank you.

[The prepared statement of John C. Browne follows:]

PREPARED STATEMENT OF JOHN C. BROWNE, DIRECTOR, LOS ALAMOS NATIONAL LABORATORY

INTRODUCTION

Mr. Chairman and members, thank you for the opportunity to discuss the security environment within which the Laboratory operated when the recent serious security incident occurred. When I first heard about this incident my reaction was probably the same as yours—how could this happen at Los Alamos after all the events of last year? I am angry and frustrated. The fact that the hard drives with classified information were found on June 16 by one of our people does not diminish accountability or responsibility to address the root causes.

We made many significant improvements to security in the last year, with a strong emphasis on cyber security. We enhanced our security awareness training for our employees and subcontractors. Nevertheless, this incident still occurred at our Laboratory, leaving us to ask what more needs to be done.

Although there are no excuses for this incident, there may be some contributing factors. The issues I have identified so far involve the adequacy of required DOE and Laboratory security procedures, human reliability in following procedures, and the oversight and acceptance of responsibility for security in special programs.

Key Messages

I have these key messages to emphasize today:

- We are accountable. Corrective actions have been taken; more are underway; disciplinary actions will be taken, subject to the immediate requirements of the ongoing criminal investigation.
- There is a need to return to more formal accountability for handling of Secret Restricted Data materials. Increased accountability will enhance the sense of personal responsibility, and reduce the opportunity for and consequences from human error.
- Human reliability programs need to be evaluated to ensure that people with access to the most sensitive information are included and that the program is effective.
- Outstanding science is essential to achieve our mission—we will fail without it—but it is not sufficient. Indifference or carelessness toward security, regardless of an individual's or an organization's accomplishments, will not be allowed to compromise our nation's interests. The National Nuclear Security Administration has a major challenge to reinforce the security culture while retaining science at its best in the National Laboratories, and they should be given the opportunity to do so.

SCIENCE AND SECURITY

Criticism of the National Laboratories recently has taken the form that security is in direct conflict with an elite scientific culture because security emphasizes keeping information from people while science flourishes in an open environment.

I reject the notion that science and security are incompatible. The tension that exists between the characteristics of security and science has been and can continue to be managed effectively. The most sensitive information in our custody—information about the design and operation of our country's nuclear arsenal—has been developed by the very scientists who are responsible for assuring that it is securely managed. More than any others, these scientists understand the information entrusted to them and appreciate the risks involved should it end up in the wrong hands. They have devoted their careers to public service in the national interest. They have demonstrated since the early days of the nuclear weapons program their ability to accomplish outstanding science and to simultaneously satisfy the requirements of effective security.

For over 50 years, our nation has been well served by the relationship between the University of California and the Department of Energy and its predecessor agencies. It is one of the longest lasting and most productive partnerships between a state entity and the federal government in our history. The University has provided an outstanding workforce to help the government solve some of its most challenging national defense problems. The challenge today and in the coming decade to ensure the safety and reliability of the US nuclear deterrent without nuclear testing is as great as any faced in our history. The University's role is as important now as ever.

Security management is a responsibility assigned to the Laboratory by the DOE through the management and oversight contract with the University of California. I would like to emphasize that as Laboratory Director, I am an officer of the Univer-

sity of California. In that role I represent the University and carry out the responsibilities assigned to it. I take that responsibility very seriously. The DOE sets the security rules within which we work. DOE evaluates our security performance through a series of programmatic and independent audits. DOE provides the financial resources to implement the security systems that are required. If resources do not match requirements, DOE sets the priorities. The University's obligations in all aspects of contract performance were made more explicit in the performance-based contract starting in October of 1993. This arrangement, which became a federal norm in that time frame, was to have clearly defined the contractor's accountability by establishing quantitative performance goals. However, in the last implementation of this process to the security function, the previously agreed-to criteria were dropped and our performance was judged solely by the outcome of the final 1999 DOE "go green" audit. This left our evaluation dependent on the auditors' criteria rather than a set of pre-established performance standards and metrics covering the major areas of security.

The University has greatly enhanced its ability to provide oversight by adding a dedicated laboratory management office in 1993 that provides an interface with the DOE on contractual issues. The UC Board of Regents has had a standing Laboratory Oversight Committee that regularly interacts with the Laboratory directors. The University of California President also has a Committee on the National Laboratories that is composed of individuals who previously served in senior positions in industry, government and academia. Recently the University of California Office of the President (UCOP) appointed a security advisory panel chaired by Adm. Tom Brooks and hired a former military security officer as UC security director for contractor oversight on these matters. The UCOP and Admiral Brooks have assembled an outstanding panel of security experts that has begun to evaluate security practices across a broad spectrum at the two UC weapons labs. This panel has not been in existence long enough to have an impact on our security performance. Committees and offices by themselves do not ensure security, but they do demonstrate the University's commitment to improvements in this area.

The Department of Energy announced on June 30 that it will begin working with the University of California to explore ways in which security expertise can be brought into the UC and the Laboratory to achieve improvements in security. UC and the Lab welcome the study and will fully cooperate with the Department. Although the UC contract might be restructured to provide external security expertise, the day-to-day responsibility for handling classified information will still rest on the shoulders of the scientists and engineers at the Laboratory. There are important lessons from our recent improvements in safety. Safety and security are line responsibilities. Additional expertise from outside can be very helpful, but it must reinforce line responsibility. This is where the day-to-day work occurs.

SECURITY DE-EMPHASIS FROM 1990-98

To understand the current situation in security it helps to review the changes that have occurred in the nuclear weapons program over the last 10-12 years.

After the end of the Cold War, the budgets for the nuclear weapons laboratories dropped rapidly. There was considerable pressure from the DOE and the Congress to reduce overhead costs, and this included security. Security funding dropped to a new low, especially for physical security.

Policies changed as well as funding. Individual accountability for classified documents was done away with as a cost saving measure across the government. Secret Restricted Data document accountability was dropped as federal policy in 1992 and by 1993 after some debate Los Alamos ended this practice. In 1997, Top Secret Restricted Data document accountability was dropped as a federal requirement by DOE and other agencies. For Top Secret material and Sigma 14 and 15 weapons data we have continued to require more accountability and control than has been required by DOE.

There were other changes as well. Significant amounts of information were declassified. The name of the DOE Office of Classification was changed to the Office of Declassification. A policy of openness was promoted that aimed to make more information available to the public, especially information related to the safety and environmental impacts of nuclear activities.

A significant change of practices was instituted in the 1994-95 time frame when we were instructed to reduce the number of Q-cleared personnel (Top Secret) by downgrading many of our employees' clearances to L (Secret). The result was many more people with lower level clearance in our secure work areas. Not long after that, distinctive colors for Q-cleared versus L-cleared badges were dropped, which made the identification of the security access of individuals much more difficult. While

none of the above changes can be shown to have a direct bearing on the hard-drive incident, they were part of the atmosphere that was created after the end of the cold war.

A few years after these budget reductions and policy changes occurred, we began having difficulty earning satisfactory ratings in security reviews and audits by the DOE. In addition, information technology was expanding at an incredible rate. Reinvestment in security began to occur, but too slowly to address the new environment.

I faced this condition when I became Director of Los Alamos in November of 1997. I began to increase our overhead funding of security to make the changes mentioned elsewhere in this testimony. We have made significant progress. We still have further progress that needs to be made, and we are dedicated to doing that.

SECURITY ENHANCEMENTS SINCE 1998

In early 1998, I provided greater emphasis on security and environment, safety, and health by creating a Deputy Laboratory Director position that would concentrate on operations, including security and safety. Previously, a single deputy director had oversight of all operational, business, and outreach functions. In April 1998 I formed a separate Security Division, reporting to my operations deputy, with a former Air Force security officer specializing in nuclear security at the head. Consequently, a greatly improved Site Safeguards and Security Plan was developed and approved by DOE—our first since 1994. In a similar manner, I created a new Counter-Intelligence office, headed by a former FBI CI expert and reporting to the operations deputy but with full access to me.

In response to last year's criticism of cyber security at the defense national laboratories (Los Alamos, Livermore, and Sandia), these laboratories and DOE developed a Tri-Lab Information Security Plan in April 1999. The Laboratory is implementing this plan, and to ensure continued coordination of these improvement efforts, I formed a senior Information Security (INFOSEC) Policy Board, headed by my principal deputy. In addition, a formal technical program was created to lead our technical efforts to identify and develop solutions to present and projected computer security challenges. This program interacts directly with the INFOSEC Policy Board to ensure tight communications regarding Laboratory objectives, priorities, and oversight. The Security and Safeguards (S) Division is represented on the INFOSEC Policy Board to ensure compliance with the security regulations and guidance issued by DOE Safeguards and Security organizations.

Cyber security upgrades in the past year include

- Strict site and cyber access for foreign nationals.
- Network separation with firewalls between Laboratory unclassified administrative computing and public information computers—an additional layering beyond complete isolation of the classified computing network completed six years ago.
- Eliminated except in very special cases authorized use of any computer for both classified and unclassified computing (dual-use computers eliminated).

Actions After The Hard-Drive Incident

As soon as the hard-drive incident was reported to me on June 1, I initiated all actions that were required, prudent to limit further damage, or appropriate to facilitate further inquiry. Those actions include temporarily eliminating SRD access for members of the NEST team who had unescorted access to the vault in question until we had a better understanding of the FBI investigation.

Some of the actions taken in June have become continuing policy, such as:

- Logging of all vault entries and exits, with positive identification.
- Reduced access lists for vaults and Limited Access Control Areas (LACAs).
- Placed barcodes on all portable high-density computer storage media with Secret Restricted Data (SRD: secret nuclear weapons data) to facilitate inventory.
- Initiated a review of all nuclear weapons programs to ensure that they have security plans consistent with DOE and Laboratory policy.

These activities addressed immediate concerns, but we recognize that more may be required. We are working with the DOE to identify and implement additional measures that address root causes.

Last year I established a Lab-wide goal of "Zero Safeguards and Security Violations." Upgrades in personnel practices to ensure suitability of staff for critical national security jobs includes intensified security awareness training, enforced by automatic rejection of personnel at entry badge readers if their training is overdue, and implementation of the DOE's counterintelligence polygraph program.

To reinforce the message of low tolerance for serious violations, strong sanctions are being taken by line managers for serious or deliberate security infractions. Since I have become Director, I have found it necessary to terminate 3 employees and sus-

pend 4 others for serious security infractions and violations. For lesser infractions, sanctions such as salary reductions and reassignment to less responsible jobs have been applied. I have also empowered my managers to pull the Laboratory badges of non-UC subcontractor workers in their organizations who had the privilege of site access but failed to follow our procedures. This action also has been taken a number of times recently for visitors who did not comply with security procedures. After the investigations are complete in the hard-drive incident, appropriate personnel actions will be taken. It is not fair to our thousands of conscientious employees to tolerate the deliberate, careless or indifferent acts of a few individuals.

Oversight

The quality of the Laboratory's security program is monitored through regular self-assessments and DOE evaluations. UC had also added detailed oversight through its new security office and panel that reports to the UC President's Council.

In the last few years we have made substantial investments to provide a stronger security environment. The improved status of our whole security posture was validated by the DOE's Office of Independent Oversight and Performance Assurance (OIOPA) at the end of 1999 with a rating of "Satisfactory," the highest of their three rating levels, following a year of preliminary visits and final audits. The GAO followup report, "Improvements Needed in DOE's Safeguards and Security Oversight" (February 2000) primarily addressed needed integration of oversight findings and followup records in DOE's methods. In this regard, the GAO report also calls out as a noteworthy practice that Los Alamos maintains its own database with "virtually every known security problem at the laboratory" as a method to track findings and corrective actions—although improvements were recommended in root cause and risk/benefit analyses.

The DOE Inspector General investigated security inspection ratings at Los Alamos for 1998 and 1999 and in May wrote the *Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self Assessment at Los Alamos National Laboratory.* Most of the report is related to DOE ALO. I will not comment on those findings.

The portion of the IG report dealing with LANL self-assessments in 1998 and 1999 alleges that a) all self-assessments were not completed by LANL as required; and b) ratings on some self-assessments were manipulated by LANL management to make the Lab look better than the facts would have indicated.

Self-assessments are a valuable internal tool to senior management because they allow us to determine where we need improvements. The DOE OIOPA audit reviewed our self-assessment function after the IG visit to LANL and found that the LANL self-assessment program was operating and communicating the results to management effectively. Manipulating self-assessments as alleged would be counterproductive to our goals of having an effective security. Self assessment findings have no direct impact on DOE's annual evaluation of our security performance.

If the DOE IG will share more information on those allegations with me, I will investigate further. It is correct that we did not complete as many self-assessments as we had planned. We went beyond the DOE requirement for self-assessments and set a "stretch goal" that we missed. However, I would like to point out the Laboratory's security program was reviewed 16 times in 1999 alone. The DOE-IG report is the only audit for which we objected to the findings, and our objections were only because the findings could not be validated.

Current Regulatory System

The regulatory system for security, like safety, is complex and multilayered. At the top level public laws provide general principles and objectives. Next, the DOE has established a layer of rules in the Code of Federal Regulations and then has a layer of requirements in their Orders system. The Orders system has many thousands of pages of orders, manuals, and guides that are under constant revision. Requirements can be modified in real time by DOE direction.

One of the contract roles for the University of California is to help, with the DOE and the Labs, review regulations as they are developed and to maintain a list of applicable requirements.

INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT (ISSM)

To deal with this complex environment we are taking the same approach to security that we took with safety. It is called Integrated Safeguards and Security Management (ISSM) and uses a simple five-step approach that every employee can understand. We are writing plain language "Laboratory Implementation Requirements" (LIRs) that capture all the government requirements in a form that allows the employees to understand what they must do in a given circumstance. Many re-

quirements are common sense and we must continue to work toward a simple system that is easily understood but is difficult to circumvent.

Ultimately, security depends on individual performance. This is not unlike the individual's responsibility for safety. With the general security objectives in mind, the logic of the rules can be followed. Following the rules offers the worker protection when some failure occurs. More importantly, we have found that formality of operations encourages work habits that prevent failures.

To reinforce these expectations, I have directed all employees to participate in mandatory security awareness training, and review their security responsibilities with their next level of supervision.

We have the experience from implementing Integrated Safety Management (ISM) over the last three years that self-reporting is an important tool for performance improvement. Self-reporting is defeated in a climate of fear. We must maintain the support of the employees for self-reporting while carrying out our responsibilities for management oversight of the lab.

Over the last five years, we have averaged around 40 security "occurrences" per year. Most of these were self-reported and were administrative security infractions that had no or minimal impact on loss of control of information. Those that were serious were dealt with swiftly. It is important that we retain honest internal reporting and self-evaluation, if we are to improve our performance in security. I would be suspicious if only a few security occurrences or safety incidents were reported in an organization of 8,000 employees. Our goal of zero security violations can only be met by honest reporting and by addressing root causes.

CLASSIFIED MATERIAL PROTECTION AND CONTROL

Security implementation includes providing secure work and storage places for classified material, controlling the movement of that material, and qualifying personnel to ensure trustworthiness, and regular training.

Physical Security

The Laboratory has several layers of physical security, providing graded protection and defense in depth around classified materials. The outermost layer is the Laboratory site boundary, which encompasses DOE property. Inside this boundary, all persons are subject to DOE rules including following guard force directions. Vehicles and personal belongings are subject to search. A professional protective force with approximately 400 armed guards enforces these rules and site security.

The next layer is the security fence. Unescorted access to the Administration Building security area (which incorporates X-Division's principal work space) is through portals using a Q- or L-cleared (secret—national security information [NSI]) badge plus identification either by a guard from the badge photo or by means of the badge plus a hand-geometry biometric reader. About 8000 people have badge access to the Administration Building. Other Q-cleared buildings have similar measures.

X-Division's principal workspace is located within a Limited Access Control Area (LACA) inside the Administration Building. The LACA is an additional layer of security that we use to identify and authorize a group of people doing related work inside a more general security area. Unescorted LACA access, through another badge reader, was allowed to about 1300 Q-cleared people who required emergency access or who routinely work in or with X-Division, usually involving Secret Restricted Data—secret nuclear weapons data. (Once inside the LACA, personal recognition provides a strong deterrent to unauthorized access.) The access list for the LACA badge readers has been pruned to 600 people.

Another higher-level security environment can be provided by a Sensitive Compartmented Information Facility (SCIF). These areas can be multi-office work areas, like a LACA, but with more extensive access control features specified in federal standards. SCIFs are normally used for intelligence work or for Special Access Programs (SAPs).

The next layer of physical security in classified workspaces is provided by personal control or secure storage of the classified materials. When not in the possession of an authorized user, classified material must be in approved storage. Approved non-work-hours storage can be a safe in an office, a vault, or a vault-type room meeting standards specific to each kind of system, its security environment, and the classification level of the material inside. The DOE standards cover the storage device location, construction, and door locks. For a vault, a GSA-approved standard lock and intrusion detection alarms are required.

Los Alamos vaults have always been equipped with GSA approved locks and intrusion alarms that meet DOE standards. Until June, workday practices for control of classified material were met by various means allowed by the DOE requirements.

For some vaults, including the vault in question, a number of Q-cleared persons were authorized for unescorted access. No entry logging process was required by DOE or the Laboratory or routinely in place when the vault was attended.

After the hard-drive incident, we immediately instituted a vault access-logging requirement that subsequently became DOE policy per Secretary Richardson's June 19 memo. We are now meeting that requirement for all of our 96 vaults on site.

Since 1994, we have had 19 DOE inspections that covered vault operations. These resulted in two findings. One finding is closed and the other, involving a technical issue regarding alarm testing, has a corrective action plan. Neither of these two findings addressed the issues surrounding this incident.

DOE is planning to review vault operations across the complex and establish upgraded standards on a very fast track. We have already reviewed the security practices at all 96 vaults at LANL. We welcome the DOE review.

Information Security

Information security is provided by physical security as described above and by controlling the movement of the information. The rules for controlling computer media have evolved to be somewhat different than for hard copy on durable media such as paper and film because the expansion of digital storage capacity challenges the traditional concept of "document." Some hard drives in personal computers can hold more than the equivalent of a million pages of text. The increase in the amount of material that can be compromised and the speed with which it can be transmitted as digital capabilities increase is a government-wide problem that must be broadly addressed. Many of our cyber security improvements of the past year were aimed at this problem and we continue to deploy technology to address what may be the most volatile security issue we face.

In 1992 when SRD accountability changes occurred, DOE was not prepared to give guidance for the secure handling of computer based information. The technology was changing so rapidly it was difficult for anyone to keep up. The computer technology moved faster than security technology or policy. We needed clearer overall guidance in order to follow priorities on expenditures. This all occurred in an environment when great pressure was being applied to reduce overhead accounts. In such an environment, it was essential that we follow DOE policy and expenditure guidance.

As said earlier, government-wide policy from 1992 ended the requirement to maintain an auditable inventory of Secret Restricted Data material. This is often referred to as the "end of accountability," but of course, everyone is still responsible for the classified documents in one's possession. The Laboratory follows DOE policy for accountability of SRD material.

Positive inventory control for all of the approximately 6 million classified items now in the Laboratory's possession raises the issue of cost vs. benefit that caused the downgrading of requirements eight years ago. We estimate that the effort to reinstate an inventory listing of all SRD items would be at least $60M. Maintenance of the accountability system plus periodic inventories would cost on the order of $25M per year.

An inventory system can help reinforce careful work habits as well as providing more positive document control. The cost and difficulties could be reduced by a graded implementation. For example, the first focus could be on inventorying portable high-density digital storage devices. We have now completed that task. Sigma categories can be used to prioritize items for inventory. Security and subject matter experts should be involved in detailing standards. It would be costly and ineffective for the Laboratory to attempt to create its own inventory system without DOE guidance. Any system must be DOE-wide to be effective. The magnitude of such an effort will raise issues of costs and benefits. DOE will need to establish priorities for resources.

Prior to this incident there was no government requirement to protect a compendium of secret information beyond the requirement that applies to the highest level of classification of any item in the compendium. This is regardless of the volume of information.

Immediately following the hard-drive incident, I directed that portable high-density digital storage devices with SRD must be put under inventory control. For this purpose, bar-coding on some 65,000 such devices is essentially complete. As announced in June, the DOE will institutionalize the inventory control requirement for selected compendia of secret information on high-density media. We strongly endorse the development of such a plan.

There is no formal DOE or Laboratory requirement associated with transfer of SRD ownership within a Q-cleared security area. In particular, the previous owner is not required to retain a record of change of ownership, so in a sense, everybody

owns it—and therefore nobody does. The opportunity to lose track of ownership is high in multi-user vaults if there is no formal accountability. This may have been a contributing factor in the hard-drive incident. Prior to the 1992 changes, the originator of a document had to record any copies made, number the copies, and the tracking system retained a record of all copies and their owners. We recommend re-establishment of rules for tracking SRD (and higher) document ownership.

Transport of SRD outside of a security area requires physical security measures, but without inventory controls, there is no unique identifier to track removal, transport, and arrival of the item. Document accountability is important when documents are transferred between owners and transported outside of the security perimeter. Tracking document transfers and movements would be enabled by and should be part of a revitalized accountability system.

With modern technology, there is an opportunity to develop centralized electronic repositories with a high degree of security, tracking, and access control. This would, however, create a security vulnerability by concentrating information. Security measures would have to be very high for such a system, but may be the best approach for a cost-effective document control system.

The digital age has created new problems for information security and may also provide means to help that should be further considered. Encryption of classified information could be an important augmentation to other security measures. Secretary Richardson directed that encryption be utilized in protection of large quantities of SRD. A limited set of software encryption tools are available now, but are likely to improve rapidly in coming years. We plan to utilize these developments in concert with DOE.

Personnel

In my opening comments I identified human reliability as one of my core concerns. This concern is widespread in security management. A recent DoD study[1] "Insider Threat Mitigation" identified maliciousness, disdain for security procedures, carelessness, and ignorance as four kinds of insider behavior that can generate security incidents. Our system attempts to minimize these behaviors by thorough selection, training, mentoring, and re-evaluation of personnel, but needs to be strengthened.

Access to various levels and kinds of classified material can be authorized to persons with corresponding clearance levels and need-to-know. Clearances are provided through the federal departments for their own personnel and contractors. Although periodic reinvestigations check external risk factors such as indebtedness for cleared personnel, it may be necessary to strengthen personnel requalification through a better human reliability program.

The 1995 DOE policy to make L (Secret) the default clearance level instead of Q (Top Secret) introduces many less-scrutinized people within our security perimeter. We recommend that only Q-cleared personnel have routine access within our security areas. This would require a much higher quota of new Q clearances.

Personnel develop sound security work habits through initial training, work experience in a supportive environment, and refresher training. This is the normal process at my Laboratory. I know these people and I know their work style. It is not an atmosphere of widespread disdain for security.

However, to ensure that current requirements are clearly understood, we conduct required periodic security retraining and hold occasional special events for security awareness. The basic retraining program has a number of elements and is largely computer-based on the Lab's internal web, to ensure currency and standardization. The retraining system is highly automated, including reminders emailed to the individuals and their administrative offices, and automatic rejection of personnel at security area badge readers if their training has lapsed.

We have conducted a number of special events for security awareness that consist of presentations by respected security experts and use of professionally-prepared training materials. This follows a pattern developed by Integrated Safety Management that has been well-accepted by the workforce. We had very good employee feedback from these sessions. I have directed that security awareness training be conducted this summer for all employees. This will be an occasion for presentation of the Integrated Safeguards and Security Management System to the whole workforce. Additional security training will be focused on areas of need; for example, last week we conducted a security immersion day for NEST.

I am particularly concerned about the apparent human failure involved in this incident. Losing or misplacing secret information is a serious matter but does not nec-

[1] *DoD Insider Threat Mitigation:* Final Report of the Insider Threat Integrated Process Team, available by subscription from http://www.insidedefense.com/

essarily expose the individuals involved to severe disciplinary action if promptly reported. The rules are intended to accommodate a certain level of inadvertent security infractions through self-reporting. Through prompt reporting it can sometimes be established that the material was never left unprotected, and if not, then its movement can reconstructed and perhaps the material can be found. With prompt action the consequent damage to national security can be more effectively determined and limited. We will have to ensure that our security awareness training strongly re-emphasizes the reporting requirement to our employees.

DOE has several special personnel programs, such as the Personnel Security Assurance Program (PSAP) and the Performance Assurance Program (PAP), to assure fitness for particular duties. For example, personnel handling nuclear weapons are evaluated for psychological stability and drug abuse. It is important that an expanded human reliability program be wisely employed to help us determine if we have risks with people in our most sensitive programs. The DoD report cited above reaches a similar conclusion.

Access to Programs

There are rules specifying access privileges to information in various categories according to the clearances held by a person. Beyond a Q-clearance, which enables access with need-to-know (NTK) to SRD and Top Secret material, there are Special Access Programs (SAPs) and Sensitive Compartmented Information (SCI) access.

SCI information is often intelligence-related and compartmentalization helps protect sources and methods as well as highly sensitive information. Access to a SAP or SCI program can be granted only by a designated government program manager. Los Alamos works in many SAPs and SCI programs with the DOE and other federal sponsors. A DOE rulebook dictates the formal steps required for in these relationships to ensure that roles and responsibilities are documented.

There are a number of special programs (non-SAP, non-SCI) at Los Alamos into which line managers have had little or no access to ensure that Laboratory safety and security rules are met. Prior to this incident it was not clear to our line management and security people whether or not they had the necessary authority to accept responsibility for the detailed security procedures of these programs. By their very nature, sponsors try to limit the number of people who have access to such programs. It is important that the line management maintain oversight of the security and safety of all such activities with assistance from security experts.

NEST SECURITY

The NEST program has been operated as a closely held need-to-know program but not a formal Special Access Program. Los Alamos has made a good faith effort to participate in this program as we understood the guidance of the program sponsors in DOE. Oversight of NEST by our Security Division was limited. Not all aspects of the NEST security plan were reviewed and approved by laboratory managers for compliance with DOE rules or for best security practices. Even if NEST was treated as a closely held need-to-know program, it was subject to DOE policy for handling SRD, and that policy was in place at the Laboratory. We have been asked by the FBI not to interview the current Los Alamos NEST team, so we cannot report on any security audits that the team may have conducted. I also do not have the results of any security audits of NEST that DOE may have conducted. However, our preliminary review of NEST operations prior to the FBI being engaged indicates to us that the program operated using normal SRD security measures, although additional factors may be uncovered by the present FBI or future investigations and could cause us to modify this judgment.

The vault where the X Division NEST toolkit was stored was subject to normal inspections by our Security Division. Since there was no accountable matter in the vault, inspections were related to physical security and spot-checks on document markings. Adequate equipment, procedures, training, and personnel qualifications were in place to enable secure handling of NEST items.

Execution of security oversight is less clear. Our discussions with DOE have revealed that some personnel at DOE did not have the same understanding as LANL personnel of how NEST program security was to be administered. Elimination of such misunderstanding is a mutual responsibility of the DOE and the Laboratory.

We believed in good faith that this program was indeed considered special in a very real sense, i.e., a "close-hold" program. There was a list of the people allowed access to the information. Deployment details were very closely held. We are addressing this issue with DOE and are working together to eliminate the ambiguity that we have discovered. In fact, the Deputy NNSA Administrator for Defense Programs sent me a letter on June 16 clarifying that we are responsible for the security of all programs unless directed to the contrary.

There are a number of other closely held need-to-know programs that have some of the characteristics of the NEST program. On the basis of the NNSA letter we are undertaking a comprehensive review of their security. I believe that NEST and other closely-held need-to-know programs should have a level of formality that includes, at a minimum, a security plan reviewed and approved by DOE and laboratory management delineating roles and responsibilities for security for all participants, strict accountability and tracking control for all SRD (and higher) information and equipment, regular security/counter-intelligence training and certification, and regular audits.

Such measures would not necessarily have prevented the hard-drive incident , but would have made it easier to detect someone violating security.

SUMMARY OF CURRENT ACTIVITY

It is critically important for national security that our recent security incident be analyzed, the lessons learned, and corrective actions taken. At the local level, many changes already have been implemented and many are planned or under consideration. At the national level, actions are underway that provide an enhanced focus on security, especially for computer media. I will summarize recommendations and actions underway.

First, the National Nuclear Security Administration will provide a new setting for our nuclear weapons programs, including a strong focus on security management. It is important that the NNSA and its new leader, Gen. John Gordon, be given the opportunity to create a new management team and processes that will ensure we accomplish our mission with effective security for these times.

I am also very pleased that the Administration has created the Hamilton-Baker panel to review the hard-drive incident. I believe that these two distinguished public servants will provide a thorough and thoughtful analysis and recommendations.

We are implementing upgrades to current security practices to address some of the underlying factors that may have contributed to the recent security incident. I have explained most of these in context above. In summary:

- Upgraded access control measures now in place include positive identification and logging of persons for vault entries by the vault custodian during work hours and through the central alarm system manned 24 hours per day by our guard force. In addition, if a vault custodian leaves his/her station, the vault must now be locked and alarmed. Entry to Limited Access Control Areas is also under review to improve controls.
- We are implementing inventory control of portable high-density data storage devices with Secret Restricted Data. Device bar-coding for this purpose is nearly complete. Development of requirements are underway with the DOE for reinstating inventory control of SRD information.
- We are also considering how to reduce the volume of secret information held in distributed storage, to facilitate inventory control, yet not lose the valuable information from the past.
- Encryption will be evaluated and incorporated as DOE guidance is received. This will preserve the secrecy of information regardless of control of the physical media.
- In our security awareness training, we will emphasize the importance of continuing self-reporting. We must ensure that our security practices do not discourage this.
- We are considering how to provide a graded approach to personnel evaluations according to their access to the most sensitive information. It may be necessary to include PSAP-like features in evaluating fitness for duty for some positions.

CONCLUDING REMARKS

If we made all these significant improvements in security over the past year, why didn't it prevent the latest security incident? It appears that there are a number of contributing factors, none of which can be or should be used as an excuse.

Policies, procedures, and security systems are all necessary to make it difficult for someone to compromise our nation's secrets, but also to make it easier to detect someone who tries to do so. Such measures will not be able to wholly prevent inadvertent or intentional human error.

There are additional improvements we can make. We will follow DOE guidance when it is received. To initiate further changes without that guidance usually leads to backing up and starting over, which wastes scarce resources.

We have worked very hard and invested many resources in physical and cyber protection, but nonetheless we have suffered severely damaging incidents.

Many people have stated that security, due to its inherent desire to keep information closed, is totally incompatible with science, whose fundamental premise is openness. There is no doubt that there is a tension between these two objectives—but it has been managed at Los Alamos and elsewhere for many years. It requires great diligence and continual improvements to deal with changing situations. It must be managed because science is too important to the future of our nation's security. Science creates the ideas that strengthen our national defense. Science created the information on the hard drives. We look forward to the leadership of the NNSA to help us strengthen our security environment while preserving science at its best.

Although we incorporated all existing DOE policies in our requirements and had highly qualified workers involved, it appears a failure to execute required duties occurred, possibly from deliberate human action or omission of action. Security is not just the rules and the systems. We must engage the hearts and minds of the people. I reject the conclusion that this latest incident is typical of our workforce. Our people are dedicated to national security. Many have spent a large fraction of their lives contributing to our most important national problems. At the same time, we must insist that arrogance, carelessness and indifference to security not be an excuse for inadequate protection of our nation's secrets, regardless of the scientific accomplishments of the individual or the organization.

Our goal is zero security violations. We are accountable and committed to make the needed changes to improve our security. We can have science at its best and security at its best. Our nation needs both and should demand no less.

Mr. UPTON. Thank you.

Dr. Tarter.

STATEMENT OF C. BRUCE TARTER

Mr. TARTER. I will try to be very brief also. Let me first reinforce and reaffirm what I think Dr. Browne has just said, that security, and I think it also restates something I think Mr. Podonsky said several times this morning, both in its testimony and in answer to questions. Security on our site is our site's responsibility, and responding to basically the set of Department of Energy requirements. It is not some third party. It is not somebody else. It is mine as the leader of the site. It is the responsibility of the employees on the site. And that is ours to do in response to DOE requirements. And I think you pointed out occasionally that comes into some degree of conflict of knowing exactly how to implement those, but that is the way the system works. There aren't magical silver bullets in the sky that you invoke to make it happen. We have to do it onsite in response to the DOE regulations and what will now become the NNSA part of those regulations.

I think, as I said to the committee last year, we have, I think, done well in many aspects of security. I think there are two that I think are still very much works in progress. And I think the committee has covered one this morning very, very thoroughly, but let me mention the two I think—one that has come out of the hearing and one which several committee members have alluded to. And as I was listening to all the testimony this morning, I was struck again and again about details of vault access, details of document control. A whole variety of different things. And you do not want to go back to one thing. But whatever the set of events that created the set of actions taken in the early 1990's, which basically took accountability of documents out—off the table, I think almost everything else in dealing with the inside treatment of information has flowed from that. And in agreement, I think with Dr. Robinson and Dr. Browne, and I believe the Department, I think we do need to return to a system of full accountability for the documents inside the system.

It is not as simple as just saying it. It is a major task. The interface with other agencies is complex. Contrary to some testimony, the Department of Defense does not have as close a security system in those documents as we had before the 1990's period. But I think we need to do that.

The second thing—and I think Congressman Cox has made this point on a number of occasions, I think when you visited this you saw this, too—that technology has outstripped, in many cases, what I would call your intuition, and our intuition, about how to treat—how to protect great masses of concentrated information of high value. And I think that is something which is still a work in progress. I think all of us appreciate the supplemental money which has been, I think, added to help us this year now to work on that problem. But this is not a simple problem, because taking all of the documents we have, we can still put them in very small concentrations, and I think we need a different way of treating that information.

Let me close by simply stating that I think there are two other comments. I think as with the other laboratories, in spite of the change in document control, we continue to treat Top Secret information differently. We have had that under almost a complete control, and I am confident that that information has been handled well over this period of time.

Second, one of the first things that I did after I was informed of the Los Alamos incident was go through our NEST procedures. I would be happy to do that for the committee, but we found everything was where it was supposed to be. And I went through our procedures, and I believe they were quite adequate. But I would agree that I believe there should be a formality of operations complex-wide because as I learned, most of our particular NEST regulations were ones that were done by our own site. I think they were good ones, but I think it should be done uniformly across this system. Thank you very much.

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

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

OPENING REMARKS

Mr. Chairman and members of the Committee, I am the Director of the Lawrence Livermore National Laboratory (LLNL). Our Laboratory was founded in 1952 as a nuclear weapons laboratory, and national security continues to be our central mission.

The specific events that prompted these hearings are most regrettable. However, I welcome the opportunity to report to you the progress we are making to increase security at our Laboratory. My statements before this Committee during the past year provide a record of the many specific actions we have taken in this area. And, in January 2000, our Laboratory was visited by three members of the Subcommittee—Chairman Upton, Vice Chairman Burr, and Representative Cox—to see our security measures first hand and to discuss issues with senior managers as well as working nuclear weapons specialists in their workplace. We were very grateful for that opportunity. These prior interactions and my testimony today focus on three points:

- **Progress.** In December 1999, Livermore's security programs received an overall Satisfactory (Green) rating from DOE's Office of Independent Oversight and Performance Assurance. Since the Los Alamos incident, we have been expeditiously implementing enhanced protection measures—those directed by DOE Secretary Richardson and those taken on our own initiative.

- **Commitment.** Our national security mission and safeguards and security are inextricably linked, and we take both obligations very seriously. I am ultimately accountable for the Laboratory's performance and have made very clear to all employees, who have been specially trained in security measures, their individual and collective responsibilities.
- **Challenges.** An extensive security and counterintelligence infrastructure is in place. However, we continually have to adjust to new security threats and challenges, and those arising from rapid changes in information technologies warrant particular attention and investment.

IMPROVEMENTS TO INCREASE CONFIDENCE IN SECURITY

A Satisfactory (Green) Security Performance Rating. Throughout 1999, we worked expeditiously to address all issues that arose in self-evaluations or resulted from the May 1999 inspection by the DOE Office of Independent Oversight and Performance Assurance. In particular, we took steps this past year to upgrade each leg of our security triad—physical security, cyber security, and personnel security (including counterintelligence). Actions included steps to improve:

- *The protection of Special Nuclear Materials (SNM),* by executing an action plan to analyze, document, performance test, and enhance the Laboratory's comprehensive protection strategy. We also made numerous physical and procedural upgrades and increased the size of our Special Response Team.
- *Procedures for Materials Control and Accountability,* by demonstrating the ability to consistently meet SNM measurement and inventory requirements and resolve inventory differences in a timely manner.
- *The physical security and protection of classified matter,* by addressing performance issues in several of our vault-type rooms (VTR), upgrading classified parts storage areas, replacing non-GSA-approved repositories, and installing additional barriers to segregate L-cleared employees from Q-clearance-only areas.
- *Cyber security,* by implementing scheduled steps in a Nine Point Action Plan to better protect both unclassified and classified computer systems. For example, the installation of a firewall between the open and restricted portions of the unclassified network has increased protection against outsider threats. For the classified system, which is not connected to the outside world except through NSA-approved encryption, steps were taken to protect against "insider" threats: ensured physical incompatibility of removable media between classified and unclassified systems, logged access to centralized weapons data bases, rigorous new procedures for the transfer of unclassified data from classified computers, and additional internal firewalls to enforce stringent need-to-know separations.
- *Counterintelligence,* by adding staff to a Counterintelligence Program at Livermore that was established in 1986 and has been well integrated into the U.S. counterintelligence community for many years. Polygraph testing of identified classes of employees has also begun and we are committed to completing the necessary testing.
- *Employee security awareness and training,* through a comprehensive security awareness program that exceeds DOE mandatory requirements. In addition, all Laboratory staff participated in two two-day stand-downs of activity in 1999 for intensive training and to review their individual and collective responsibilities.

As an outgrowth of these efforts, we received an overall Satisfactory (Green) rating from the Office of Independent Oversight and Performance Assurance in their Follow-up Inspection in December 1999. We continue to make upgrades to strengthen all aspects of security, address identified issues—such as those that arose because of the Los Alamos incident—and deal with any perceived weaknesses.

LLNL Actions Following the Los Alamos Incident. Lawrence Livermore personnel also support emergency response activities such as the Nuclear Emergency Search Team (NEST). In conjunction with this responsibility, the Laboratory has classified hard drives and computers that are taken to the field to complete assignments as requested by DOE. Livermore officials were made aware of the security incident at Los Alamos as soon as their top management was informed. We conducted our own, parallel review at Livermore to assure that our emergency-response assets had not been compromised. All NEST data stored at the Laboratory was and is accounted for.

Beyond NEST, the incident raised broader issues about access to vaults and portable, highly-concentrated collections of sensitive data at Livermore. A working group was immediately chartered to review the Laboratory's classified data holdings, identify the locations of especially sensitive and portable collections of high concentrations of data, and recommend appropriate procedures to provide additional protection. This review has been completed and found that we were compliant with DOE

requirements. Nonetheless, enhanced chain-of-custody controls and access procedures have been implemented at the identified locations.

Access control to vaults and vault-type rooms (VTR) at the Laboratory is managed in accordance with current DOE requirements. An access control list is maintained for each, and an area custodian uses the list to determine who may enter without an escort. We are upgrading our vault-access verification procedures in accordance with the Enhanced Protection Measures directed by DOE Secretary Richardson on 19 June 2000. In addition, the Laboratory has instituted a working group to address the effectiveness of our vault and VTR operations and management. They are in the process of identifying additional protection measures beyond those required by DOE that can further enhance security.

A Review of Classified Matter Protection and Control Procedures. Following the Los Alamos incident, the DOE Office of Independent Oversight and Performance Assurance conducted a review of the effectiveness of Classified Matter Protection and Control (CMPC) procedures at the Laboratory. The review focused on the protection of the most sensitive classified assets—weapons design information and use control information—within the Defense and Nuclear Technologies Directorate and Top Secret information. Key aspects of protection, including information generation, storage, marking, destruction, and control of access, were examined. Particular attention was devoted to the role of Laboratory management in ensuring that DOE policies related to control of classified matter are established and implemented.

The review was conducted from June 19 through June 21, 2000, and the results—as summarized in the draft report—were satisfactory. Particular mention is made of strong management attention to issues, including a proactive approach to emerging needs to enhance protection, attention to training programs, inclusion of security considerations in personnel performance evaluations, and pursuit of an enhanced security self-assessment program.

AN INSTITUTIONAL COMMITMENT TO SECURITY

Security and Science. Security and science are both central to Livermore's purpose and its operations. They are tightly coupled in our programmatic activities, and we are deeply committed to both. Through the Stockpile Stewardship Program, we further national security by applying advances in science and technology to maintain the nation's nuclear stockpile in the absence of nuclear testing. With less than 2% of the world's research and development being conducted at DOE national laboratories, many of the scientific advances that we adapt and apply to national security problems are made elsewhere. Hence, we interact with the broad science and technology community to be cognizant of major advances and to acquire needed special expertise. We also engage foreign nationals as part of our national security mission through participation in international efforts to prevent the spread of nuclear weapons, materials, and know-how.

Accomplishing our mission depends critically on these external interactions, and we must manage them in a way that protects sensitive information. It is a challenge, but not the "clash of cultures" that is so often portrayed. Since the Laboratory's founding, both security and science have been central to our "culture." The staff at Livermore take great pride in their scientific and technical accomplishments. They are also attracted to the Laboratory and are motivated by the opportunity to serve the nation. Few groups of people in the world are more painfully aware than Livermore employees what the loss of nuclear weapons secrets means to the security of the nation. Few groups are more concerned about the impact of the diffusion of information on proliferation. Few have been more at the forefront of initiatives to limit the spread of weapons of mass destruction and to develop capabilities to prepare the nation to deal with the threat of their use.

Security is not just our business, it is part of the way we operate, but so are outside technical interactions. Security and science are not incompatible objectives, but they require threat awareness, proper training, and vigilance.

Security Awareness and Training. As I have said, I am ultimately accountable for the Laboratory's security performance, and our success depends on the vigilance of everyone—from senior managers to individual employees. Increased vigilance is evidenced by a three-fold reduction in the number of security infractions that have occurred over the past year. All Livermore workers are aware of the "zero tolerance" policy for security violations that place nuclear secrets at risk. They rely on a comprehensive Safeguards and Security Awareness Program at the Laboratory to understand their responsibilities, proper procedures, and best practices. In addition to a series of DOE mandatory briefings—many of which are annual requirements—the Laboratory offers nearly a dozen additional programs, some of which train people

for specialized security responsibilities. Each year, all employees are required to complete security refresher training, and those that do not or fail the follow-on test have their clearance suspended or lose it.

As an example of training, regardless of previous assignment, employees joining the Defense and Nuclear Technologies Directorate are required to be thoroughly instructed as to their responsibility for protecting classified matter as well as specific procedures used within the program to generate, use, store, transmit, and destroy classified material. Significant additional training is required for classified-document administrative specialists and custodians.

Laboratory-Wide Implementation of Security into Day-to-Day Activities. Our institutional commitment to security is reflected in the way that we centralize authority for key functions while distributing responsibilities for execution. For example, we established in 1991 a Classified Document Project Office (CDPO) to provide Laboratory-wide programmatic direction and oversight of classified document protection and control. Interfacing with all levels of Laboratory management, the CDPO ensures development of protection and control procedures, develops and implements training activities, performs self-assessments, and manages the Livermore Administrative Document System (LADS). LADS is a centralized computer system that provides modified accountability (tracking access to material rather than specific pieces of paper) for all classified documents at the Laboratory except those that are in Special Access Programs or are in Sensitive Compartmented Information Facilities, which have additional restrictive controls.

In the area of cyber security, the Laboratory has a Chief Information Officer (CIO). The CIO leads a Laboratory-wide Computer Security Council that reviews the Computer Security Program and approves computer security policies. Program products include policies and guidelines that locally implement DOE's Computer and Telecommunications Security Orders, templates to assist the development of system-specific security plans, and checklists and testing guidelines to support certification of classified computer systems. In addition, an individual in each directorate serves as the central point of contact for cyber security. These Directorate Cyber Security Officers, who meet regularly with the Computer Security Program, oversee and ensure uniformity of Cyber and Telecommunications Security implementation. This system of Cyber Security Officers has been in place for the last six years.

University of California Actions to Enhance Security. As the Laboratory has developed and continues to develop plans for and implemented changes to enhance confidence in security, we depend on outside review to help surface the best ideas and provide quality assurance. We have benefited considerably from the efforts of the University of California Office of the President. In addition to hiring a security expert, retired Air Force Colonel Terry Owens, to serve as UC Director for Safeguards and Security, the University formed a Laboratory Security Panel of the UC President's Council. It was able to attract highly respected counterintelligence and security experts to participate. The panel, chaired by retired Rear Admiral Thomas A. Brooks III, is helping us to identify potential security weaknesses and develop improvements. Just last April the panel conducted a high-level review of our computer security program.

The University's commitment to work with the DOE to improve security at the two laboratories is further demonstrated by the specific actions UC has taken since the Los Alamos incident. In addition, since early this year, UC and representatives from the laboratories have been pursuing an initiative to develop and implement an Integrated Safeguards and Security Management System (ISSM) at both Livermore and Los Alamos national laboratories. This system, when in operation, will fully integrate security awareness, the principles of sound security practices, and the needed tools into the day-to-day performance of individuals and institutional activities.

CHALLENGES IN THE CONTROL OF CLASSIFIED INFORMATION

Accountability of Classified Materials. Accountability requirements for classified restricted data documents go back to the days of the Atomic Energy Commission. At first, these requirements included tracking and keeping precise inventory of specific pieces of paper by document and copy number. As copying machines multiplied the number of documents and copies, the inventory requirement was dropped in the late 1970's and then reinstated in the late 1980's. With changing missions and decreasing budgets, DOE aligned with the requirements of the NISPOM (National Industrial Security Program Operating Manual) and moved away from full accountability in 1992. Basically, it was concluded total accountability does not necessarily translate into total control and effective protection of the material in an age of copying machines and FAX machines. An unfortunate consequence of the change

is that it created an overall environment in which the formality of handling classified information has been reduced.

In some areas—the handling of Top Secret documents and Sigma 14 and 15 weapons data—Livermore has continued to follow more stringent than DOE-required control procedures. Greater accountability and control of such materials system-wide may be warranted. Major concerns also arise because of the revolutionary changes that have occurred in information technologies. Accountability of pieces of paper is a far different issue than accountability of hard drives that can hold Gigabytes of data, roughly a thousand times more than the main memory of the Cray-1 computer, the Laboratory's most capable machine in the late 1970s. As recent events make it very clear, we need to enhance controls over and the accountability of portable, highly-concentrated collections of sensitive data. We are taking steps to do so.

The Need for Investments. Security upgrades do not come without cost. For example, at Livermore, resources devoted to our Computer Security Program increased from $1.3 million two years ago to $18.4 million this year. To implement the cyber security upgrades that we are expected to complete over the coming year without seriously eroding programmatic work, additional funds—beyond what was in the President's budget request—are needed. This is a DOE Defense Programs complex-wide issue that merits serious attention. Adequate funding must be complemented by a consistent set of policies and thoroughly vetted planning to make certain that costs and benefits are carefully weighed as we deliberate about new directives and revised procedures.

CLOSING REMARKS

I appreciate the opportunity to address the Committee on our efforts to increase security at our Laboratory and to enhance the control of classified information based on the painful lessons learned from the recent security incident at Los Alamos. As I have stressed, secure operations are vitally important to Livermore—they underpin all our research and development activities and protect some of our nation's most closely held secrets. We continue to upgrade physical security, cyber security, and our counterintelligence program to strengthen these areas, address new threats and concerns, and deal with any perceived weaknesses. Our efforts are made more challenging by rapid changes in information technologies and would benefit from an infusion of new investments—particularly directed at cyber security.

Mr. UPTON. Mr. Aftergood.

STATEMENT OF STEVEN AFTERGOOD

Mr. AFTERGOOD. Thank you, Mr. Chairman. Thank you for holding this hearing. We have been talking not about security as much as about the rules for security. And I think that is an important distinction that has gotten lost.

GAO presented a list of rules that have been modified over the past 10 years in the direction of relaxing security. They did not ask whether those rules, in their prior form, had actually been implemented. I provide some evidence in my written statement that such rules were not implemented, in particular, annual inventories and others.

A deeper question is whether the rules were tighter or not and whether they were implemented or not? Was security better or not? An investigation done in 1990 found that there were over 5,000 Secret restricted data documents that were missing and unaccounted for. It is at least a logical possibility that security is better today, not worse, than it was 10 years ago. And because we have been focusing on the rules and not the reality of security, we are missing that important possibility.

Let me just skip very quickly. Dr. Robinson mentioned a few words critical of the declassification program of the 1990's. I would like to suggest to you that declassification is not a problem, but it is part of the solution. It is how we take this vast mass of classified information and turn it into a tractable management problem. We

are always adding stuff to the mountain of classified material. It is important that we have an orderly process to remove information control.

Congressman Cox spoke about the polygraph tests, the scientists wearing buttons. I would suggest to you that the scientists are well within their rights. Polygraph has not been proven as a useful device for employee screening. There is some data that the polygraph is useful for incident-specific investigations. In other words, to investigate a particular security violation. There is no documentation to support polygraph testing for employee screening.

You may recall that Secretary of State George Schulz famously threatened to resign during the Reagan administration rather than undergo polygraph testing. It wasn't because he was a scientist or indifferent to national security, but because the polygraph is a problematic and dubious technology.

Last, I would just like to stress the point about balance. Balance is not a word that has been mentioned much today, I think until Dr. Browne mentioned it. It is a mistake, I believe, to look at security in isolation. Security is part of a larger picture. The larger picture is the health and vitality of our national laboratories. And whenever we think about changes to security, we should ask at least two questions: What would those changes cost financially, and more important, what will their impact be on the viability of the laboratories?

You know, the Department of Defense has research laboratories also, and we do not hear any complaints about security there. The problem is we do not hear anything good about them either. Army General William Odom, many of you know I am sure, has actually called for the DOD research labs to be abolished. He said they haven't invented anything of value for years and years. That should not be our goal for the DOE national laboratories. Security is an important part of the picture, but it is only a part. And we should always think about the larger picture. Thank you very much.

[The prepared statement of Steven Aftergood follows:]

PREPARED STATEMENT OF STEVEN AFTERGOOD, SENIOR RESEARCH ANALYST, FEDERATION OF AMERICAN SCIENTISTS

My name is Steven Aftergood and I am a senior research analyst at the Federation of American Scientists (FAS), which was founded in 1945 (as the Federation of Atomic Scientists) by Manhattan Project scientists at Los Alamos. FAS performs policy research and advocacy on a range of national security policy issues, with an emphasis on nuclear arms control. I direct the FAS Project on Government Secrecy, which studies government secrecy and information security policies, and generally advocates a reduction in the scope of the national security classification system. As required by Committee rules, I hereby state that neither I nor FAS has received any federal grants or contracts that are relevant to the subject of this hearing during the current fiscal year or the two preceding fiscal years.

BALANCING COMPETING INTERESTS

The basic conundrum for information security policy is how to balance security with other competing interests such as cost and mission performance. Security is "too good" if it precludes or significantly interferes with achievement of program goals. And since funding resources are finite, there are practical limits to security in any case.

It is necessary to accept the fact that there can be no absolute security. The best one can aim for is to *manage* the security risks, keeping them to a reasonable minimum, while optimizing mission performance and limiting costs.

The proper balance is not obvious, because it depends on multiple considerations, including threat level, resource availability, and other factors, all of which may change over time. In practice, a different balance has been proposed at different times over the last decade. Some benchmarks of shifting security policy positions, as they apply to document "accountability" and classification, follow.

a. The 1990 Freeze Report: Thousands of Unaccounted-For Secret Documents

In 1990, DOE conducted a major review of security policy, which raised many of the same issues of accountability for classified documents that have recently surfaced. The Report of the Secretary's Safeguards and Security Task Force, chaired by Major General James F. Freeze, USA(ret.), noted that DOE document accountability requirements had come and gone and come again:

> Historically, the Department had not required Secret document inventories except for weapons data, and the Task Force was advised that requirement had been dropped "in the early 1970's for cost benefit reasons." However, weaknesses in the accountability for Secret documents were identified by a Classified Document Control Action Team in late 1986. Therefore, the requirement to conduct an "initial inventory" of Secret documents was included [for both Department elements and contractors]...

This new Secret document inventory requirement was not fully implemented. Even so, a partial inventory revealed that thousands of Secret documents were accounted for:

> Failure to complete the required complex-wide 100% inventory of Secret documents on a timely basis has resulted in an unsatisfactory condition... The estimated number of Secret documents throughout the complex was 6,165,969. The number of documents inventories at that time [October 1989] totaled 3,299,936, and **there were 5,716 unreconciled or unaccounted for documents.**

Interestingly, control of Top Secret documents was found to be satisfactory. No Top Secret documents were unaccounted for.[1]

b. National Industrial Security Program Eliminates Secret Accountability

The National Industrial Security Program arose in response to President Bush's National Security Review 25 (4 April 1990). It was an attempt to develop uniform security policies for government contractors in the interests of cost efficiency. As President Bush put it: "The development of a single, coherent and integrated industrial security program should be explored to determine the extent of cost savings for industry and government while improving protection of our national security interests."

In the early post-cold war days, cost savings were given higher priority than improved protection, and requirements for Secret document accountability at contractor facilities were soon dispensed with. (Secret document accountability within most government agencies had been abandoned decades earlier.)

A DOE security official articulated DOE's opposition to document accountability at a 1993 meeting of the NISP steering committee:[2]

> Ed McCallum, DOE, advised that DOE does not concur with retention of SECRET accountability, stating that it is very expensive to account for SECRET when such a security requirement can so easily be circumvented. Moreover, Ed stated that in his opinion, such a security requirement dictates that an inspector spends a good portion of their time in an inspection "chasing paper," rather than concentrating on the real security vulnerabilities at the facility.

The Central Intelligence Agency representative at the meeting also expressed opposition to accountability for Secret documents. The Defense Department favored accountability, but "with a more liberalized approach to the administrative methodology employed by the contractor." Ultimately, a requirement for Secret accountability was eliminated government-wide by the National Industrial Security Program Operating Manual, published in 1995.

c. The Higher Fences Initiative: Increased Classification for the Most Sensitive Information

In 1993, then-Energy Secretary Hazel O'Leary established a "Fundamental Classification Policy Review" (FCPR), a comprehensive review of all DOE classification policies that was intended "to determine which information must continue to be protected and which no longer requires protection and should be made available to the public." It was endorsed by Congress in the conference report on the FY 1994 En-

---

[1] Report of the Secretary's Safeguards and Security Task Force (the "Freeze Report"), December 1990, pp. 17, 70-71, emphasis added.

[2] Minutes of the NISP Steering Committee Meeting of 20 July 1993 (unpublished).

ergy and Water Appropriations Act. This was the first comprehensive review of DOE classification in fifty years, and was conducted by government scientists from DOE and DoD. To my knowledge, no other government agency has undertaken a comparable review of its own classification policies.

Along with numerous recommendations for declassification, the Review also include a call for *increased* classification of 137 categories of certain highly sensitive nuclear weapons information.[3] This recommendation became known as the Higher Fences Initiative, since it envisioned higher, Top Secret security "fences" around a small, select subset of very sensitive information. [It may be noted that any such upgrade to Top Secret would entail document accountability for the affected information, among other increased protections.]

Contrary to some erroneous news reports, the recommendations of the FCPR were accepted by Secretary O'Leary and formed the basis for ongoing negotiations with the Department of Defense beginning in 1997. However, the proposal to upgrade certain Secret information to Top Secret was rebuffed by DoD for cost reasons, even after DOE had significantly shortened the recommended list of 137 topics. DoD explained its opposition to Higher Fences in a 1999 letter:[4]

> Even working with this significantly shortened list, we anticipate that the costs of implementing such a program would be substantial. They would extend to such requirements as the upgrade of clearances with Single-Scope Background Investigations, the establishment or addition of TOP SECRET storage facilities at government and contractor facilities, the sanitization of SECRET-level computers and computer networks where this information currently resides and institution of new TS-level capabilities, etc...
>
> In addition to purely financial considerations, the DoD is concerned that there may also be operational costs. For example, the ability to respond to urgent stockpile problems may be inhibited if it should happen that the necessary responders are not cleared at the appropriate level...

This DoD assessment provides a vivid illustration of how security professionals may balance the competing interests of security, cost, and ease of operational use in different ways. Neither DOE nor DoD is obviously wrong, nor is either agency clearly derelict or oblivious to security. They have simply reached different, and conflicting, professional judgments.

(It should be noted in passing that DOE's Secret-Restricted Data [SRD] category is comparable in some respects to "ordinary" [i.e. non-Restricted Data] Top Secret elsewhere in the government. So, for example, the "Q" clearance required for access to SRD is approximately as rigorous as the Top Secret clearance. For that reason, DOE relies heavily on SRD and has rarely used the classification category "Top Secret Restricted Data," which entails security measures beyond those required for ordinary Top Secret elsewhere in the government. The 1990 Freeze Report found that there were no more than 3,451 Top Secret documents throughout the entire DOE complex, a comparatively minuscule number.)

DECLASSIFICATION AS A SECURITY MEASURE

Neither the declassification measures nor the classification upgrades recommended by the Fundamental Classification Policy Review have been fully implemented by the Department of Energy. Both aspects of the Higher Fences Initiative deserve continued consideration.

Since the need for increased protection may seem obvious at the moment, I would like to stress the equal importance of relaxing protection in areas of lower sensitivity, i.e. declassification.

There is a tendency among some to believe that greater secrecy translates directly into greater security, and that declassification means increased vulnerability. This is not so.

Declassification is an indispensable component of a rational information security program. Removing information that is obsolete or no longer sensitive from security controls through declassification keeps security focused where it is most needed. It also preserves the credibility of classification, which can otherwise become simply a bureaucratic habit, instead of a vital instrument of national security. Any information security reform program that does not provide for appropriate declassification is incomplete.

---

[3] Report of the Fundamental Classification Policy Review Group, Dr. Albert Narath, Chair, unclassified version, December 1997, page 26. An initial draft report was published for public comment on February 1, 1996.

[4] Letter to General Eugene E. Habiger, Director, Office of Security and Emergency Operations, U.S. Department of Energy, from Hans Mark, DDRE and Arthur Money, ASD(C3I), Office of the Secretary of Defense, December 17, 1999.

NUCLEAR SECRECY IN PERSPECTIVE

The Department of Energy should make every reasonable effort to ensure the protection of sensitive nuclear weapons information. But no more than a reasonable effort. The limits of what information security can achieve should be understood by everyone concerned so that responsible security policies can be formulated and implemented.

In the first place, it should be obvious that information is only one ingredient in nuclear proliferation, and it is not the most important one. No nation or sub-national group can use classified information to build a bomb unless it also has access to sufficient quantities of suitable nuclear material, and an engineering and manufacturing infrastructure to produce the bomb. But if it has the latter two items—the nuclear material and the engineering capacity—then it can dispense with classified information.

Thus, "Access to classified information is not necessary for a potential proliferator to construct a nuclear weapon," according to a 1995 report of the National Academy of Sciences.[5] This is partly due to the fact that much information about nuclear weapons design has been declassified since 1945, and partly due to the fact that such information, classified or not, can be independently replicated.

Fundamentally, it is not within the power of any classification system or any information security policy to prevent the proliferation of nuclear weapons. The most that classification of scientific or technological information can generally accomplish is to delay the independent achievement of any particular scientific discovery or technological feat. But discovery or duplication cannot be prevented.

Thus, according to a DOE report, "The considerable progress of Iraq toward becoming a nuclear power was largely independent of U.S. classification policy."[6]

Finally, everyone should understand that the number of nuclear weapons secrets is diminishing and will, in time, approach zero. The "economics" of nuclear secrecy favor disclosure, not continued secrecy: Secrets that took hundreds of person-years and billions of dollars to invent can be disclosed by a single individual and disseminated around the world in an instant at no cost—whether through official declassification, independent discovery, foreign disclosure, espionage, malice, dissent, or error. In short, it is far easier to disclose nuclear secrets than to create them. And unlike the secrets of diplomacy or intelligence, nuclear secrets are not replenished on a daily basis. There aren't many fundamentally new ones being created. As a result, we must anticipate that, whether in five years or twenty-five years, there will be no appreciable nuclear secrets left to protect. Some would say we are there already.

CONCLUSION: ENDS AND MEANS

Information security is a means to a larger end, and is not an end in itself. The frustration generated by recurring security failures at the weapons labs tends to obscure this distinction. So, for example, a proposal recently offered in the Senate would "short-circuit" the necessary balancing of security, costs, and mission performance discussed above by simply declaring that "the protection of sensitive and classified information" should be "the highest priority of the National Nuclear Security Administration."[7] But in the real world, the NNSA must have higher priorities than protecting information. Sometimes, one or more of its mission priorities—including the promotion of international nuclear reactor safety and nonproliferation, for example—will require the sharing or disclosure of classified information, not its protection.

The biggest risk of all concerns the institutional health of the DOE national laboratories. Whether one is committed to stockpile stewardship, to deep cuts in the U.S. nuclear arsenal, or to dismantlement and eventual abolition of nuclear weapons, the availability of a cadre of skilled nuclear weapons professionals is a prerequisite for the foreseeable future. These professionals are becoming an endangered species, and the laboratories are becoming a deeply unattractive place to work.

Whatever the defects of current security policy, and whatever reforms are ultimately determined to be necessary, the viability of the national laboratories is an

---

[5] "A Review of the Department of Energy Classification Policy and Practice," National Academy Press, 1995, p. 19.

[6] "Classification Policy Study," prepared for the Department of Energy by Meridian Corporation, July 4, 1992, p. 35.

[7] "Implementation of Security Reforms at the Department of Energy," a sense of the Senate resolution introduced by Senators Kyl and Domenici, June 21, 2000, Congressional Record, pp. S5573-4.

even larger and more important issue. The labs should not be sacrificed in the name of an unachievable absolute security.

Mr. UPTON. Thank you very much as well.

We will now proceed to rounds of questions like we did with the first panel of 5 minutes for each member.

Lab directors, Drs. Robinson, Browne and Tarter, what authority did you have as individuals in terms of overseeing the NEST security at your particular labs?

Dr. Robinson? We will start and go in order. Do you have a direct chain-of-command link in overseeing in terms of what they did in security?

Mr. ROBINSON. Certainly all the activities conducted on my site, I am directly responsible for including the security and the operations.

When the NEST team is deployed to the field, they must operate under the rules of the particular site. We, thank God, have mostly deployed them for exercises at other sites, rather than actual threat conditions. They operate under the site rules at that site under those conditions.

Mr. UPTON. Dr. Browne?

Mr. BROWNE. My answer would be very similar. I am responsible for all activities at the laboratory. I think in the case of this particular NEST program at our laboratory, I did uncover some issues that I believe could have contributed to the particular incident. One of those was that in looking at the security plans that were in place, they are pretty explicit that people are supposed to take care of the information, according to DOE Secret restricted data rules.

What was missing for me personally was that there was no cross-cutting NEST security plan. There were pieces of security plans. There was computer security plans, et cetera. There was no signature on those computer security plans or other security plans of any line manager of my laboratory. That is not typical of how we would run a program. Someone in line management who is responsible for the people, the facilities, would be in the chain of command for ensuring that the practices of the activities of the people were being actually followed. So I think that may have been a shortfall.

Mr. UPTON. You did not know about those shortcomings until it was discovered that the two hard drives were missing?

Mr. BROWNE. That is correct.

Mr. UPTON. Dr. Tarter.

Mr. TARTER. Again, a very similar answer on our site. I am responsible. We are responsible for the security process. I think our NEST program people had a set of procedures, both for having personnel within the program, for having them vetted for the program, for having the spectacular security things that we implemented on the site. On-site, of course, they are under the direction and the rules of whatever site they do their work within.

Mr. UPTON. Can you also tell me the differences in functions, if there are any, between the NEST teams at each particular lab?

Mr. ROBINSON. Let me go first. I think ours are the most unique. Sandia's responsibility concentrates on the arming devices, the electronics and how one might overcome those, rather than the nu-

clear design. Consequently, we had no analogous cores for NEST in any of our vaults.

Mr. BROWNE. We have several functions in the NEST program. One is a group of people who are very good at measuring radiation so that one can detect the presence of nuclear devices and determine what might be there. There are also some people who are good about analyzing how one might—not disarm but disable a device. And the third party is the device assessment team. That was the team that was involved in the X Division incident in the loss of the hard drives.

Those are the people that one would turn to to evaluate if you found an unknown object in the field—what it was.

Mr. TARTER. Essentially identical with Los Alamos.

Mr. UPTON. General McBroom, what type of relationship did you have in establishing the security of the NEST team? And specifically, why—you know, again, I mentioned this in the first panel, I would—it would seem to me that there is no data—there is no data more important than what was on those hard drives that were missing and how in the world could it possibly be classified as Secret versus Top Secret?

Mr. MCBROOM. Yes, sir, I not do classification, although I am going to take a course in it so that I can do it in the future. I would like to make those calls. We are looking at an equipment guide that we are going to put out pretty soon, which will classify all the equipment which we deal with in NEST. But I really can't address the equipment on the hard drive. Those are classified at the site and primarily with the scientists and with the security people.

Mr. UPTON. And to answer the second part of the question, what type of oversight did you have working with the lab directors to try and ensure——

Mr. MCBROOM. Oversight at the lab is lab daily business. They may have 40 different programs or 50 different programs going on there. They can't have 50 different people trying to manage everything. There is a comprehensive lab program that manages all equipment, all security; they do the training, they do everything at the lab. Now, when they deploy to the field, then we provide some oversight, but they still use the procedures from the site.

Mr. UPTON. So did you feel removed then from the security aspect of the material that they use?

Mr. MCBROOM. Well, to some degree, because my focus is emergency management. My title is director of emergency operations, so what I do is handle an emergency. In handling that emergency, I look at security, safety, all of these things as normal course of business. But that is not my focus. I am more worried right now about Los Alamos floods than I am anything else.

Mr. UPTON. How about their fire?

Mr. MCBROOM. I was worried about that when it happened, sir. Now it's all burned up and it is not going to be a problem.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Well, it will be a problem with flooding because of the pollution that is there, and it is going to affect the river and the streams and everything else around there, correct.

Mr. MCBROOM. It could be a big problem. I am heading out there next week.

Mr. STUPAK. General Habiger, you indicated that you were going to provide a time line. You had those minimum controls up there and you said you wanted to show how DOE developed though time lines, you could provide a time line?

Mr. HABIGER. That was my request of GAO. If GAO were to go look across the government, you would see that we lagged the rest of the government.

Mr. STUPAK. By "rest of the government," NSA, CIA? Labs?

Mr. HABIGER. State, Defense, yes, sir.

Mr. STUPAK. Because we are all under this one national security standard that came up in 1988, 1990 I think it was implemented?

Mr. HABIGER. Yes, sir.

Mr. STUPAK. So that was the impetus for these minimum controls?

Mr. HABIGER. Yes.

Mr. STUPAK. Regardless—I will direct this to the lab directors—regardless of what minimum controls at the labs may be under, there is no reason to lose documents or hard drives, is there? That does not fall under some minimum control saying that it is okay to lose these; right?

Mr. ROBINSON. Of course not.

Mr. STUPAK. Okay. So we can't blame these time lines or minimum controls for what happened?

Mr. BROWNE. Correct.

Mr. STUPAK. Were the labs—excuse me, the University of California, were they involved in this one national security standard? Do any of you gentlemen know that?

Mr. BROWNE. In setting the standards? Not to my knowledge, I don't believe they were involved at all.

Mr. STUPAK. Okay.

Dr. Browne, how long is a contract usually?

Mr. BROWNE. It is a 5-year contract.

Mr. STUPAK. So the earlier testimony about the Secretary, average lifetime of a Department of Energy Secretary being less than 2 years, that wouldn't impact your contract in any way, would it?

Mr. BROWNE. Well, the contractual relationship is usually handled by more than just the Secretary. There are people in the Department who have the continuity between various contracts.

Mr. STUPAK. So the change in Secretary really doesn't affect the continuity of that?

Mr. BROWNE. Not directly. It can, I guess, depending on the Secretary's personal interest.

Mr. STUPAK. And the University of California, if my memory serves me right, has had these contracts for the last 50 years; correct?

Mr. BROWNE. That is correct. 47 years at Los Alamos.

Mr. TARTER. 48 years.

Mr. BROWNE. 57 at Los Alamos. Excuse me.

Mr. STUPAK. In those contracts it talks about security, do they not?

Mr. BROWNE. The most recent contracts that I have looked at which date back to 1992, it is explicitly called out in the contract.

Mr. STUPAK. For security?

Mr. BROWNE. That's correct.

Mr. STUPAK. So if there's been a problem with security, we can't blame DOE, we can't blame U of C, we have security responsibilities that we all have to adhere to; correct?

Mr. BROWNE. That's my opinion. We all must share responsibility for security.

Mr. STUPAK. Well, in the short time that I have been on this subcommittee now, 6 years, it seems like we are always back here talking about security at labs. So we just can't blame DOE, the labs have to share some responsibility here too.

Mr. BROWNE. Absolutely.

Mr. STUPAK. Okay. And if the hard drives were missing at the end of March, it would appear that they were not lost in the confusion of the fire then at Los Alamos.

Mr. BROWNE. That's correct. I don't think you can blame this incident on the fire.

Mr. STUPAK. Okay. Mr. Glauthier, in June, I and six other members of this subcommittee asked the Secretary to terminate the contract with the University of California for the Los Alamos Laboratory because of its repeated security and other violations, and, frankly, its refusal to take responsibility for or to fix the problems. This contract has never been up for bid. I think we have established today it's 47, 48 years. But from your testimony it sounds like the Department is going to make some cosmetic changes and let UC continue on. Am I reading it properly?

Mr. GLAUTHIER. No, we believe that this is a significant change. The current contract at Los Alamos I think is 57 years, the director said. And what we are going to do now is a change. For the first time, we are going to have another firm be responsible for the security and probably some of the other industrial-type practices at the site.

I do want to be clear, though, that that is not to relieve the university or any of the laboratory employees from their responsibility to also take the proper care of secure information, classified information and materials and the like. But the practices of who is inspecting the vaults, who is actually being sure that the procedures are being carried out properly——

Mr. STUPAK. But if you are going to have a separate firm or separate entity be involved with security operations, which UC does not control or is responsible for, it sounds like it's just really another disaster waiting to happen. How is this new firm, entity, going to really carry out the mandates of the Department or what Secretary Richardson wants and what GAO pointed out? It seems like there is an atmosphere within these labs that just doesn't do it. How is another entity going to fix that?

Mr. GLAUTHIER. Well, the atmosphere is necessary to deal with no matter how security is done. What we are talking about with this firm is some organization to actually have a targeted responsibility to see that the requirements are sensible, appropriate ones at the site, follow through, make sure they are being implemented. We talked earlier about implementation. We need to see that they are actually being carried out. There are several models and the Secretary——

Mr. STUPAK. Who is going to carry them out, this new firm or UC?

Mr. GLAUTHIER. The responsibility for actually performing security is going to be one that individual scientists will have to have. For example——

Mr. STUPAK. So University of California, then?

Mr. GLAUTHIER. If the scientist has got a classified document, that person is responsible for putting it in the right place at the end of the day or transporting it in a proper way.

Mr. STUPAK. If I am a scientist and I work for UC and I am responsible for this document and I am responsible for it and I am there, and this other firm or entity comes in and tells me to do something different, who would I look to then as the scientist? Am I supposed to listen to the so-called new security entity who I have no contractual relationship with, who I can say buzz off because you have nothing to do with my evaluation, or do I listen to UC?

Mr. GLAUTHIER. First of all, we are not sure whether there will be a contractual relationship or not. That is part of what Under Secretary Gordon will be looking at over the next several months, whether this ought to be a subcontract to the university, a joint venture, or separate contracts. All of those models are on the table. But the management of the university at the laboratory will be responsible for seeing that all of its employees are carrying out procedures. They have the line responsibility to make sure it's all being managed properly.

Mr. STUPAK. Have you discussed this with Dr. Browne?

Mr. GLAUTHIER. Yes, we have.

Mr. STUPAK. Any comment on it? This other entity?

Mr. BROWNE. My opinion is that whatever mechanism the Department of Energy comes up with, we are still going to ultimately be responsible because we not only have the information, we create the information. The scientists are creating the information that winds up on the hard drives or pieces of paper. So we can't get away from that individual personal responsibility at the working level or at the management level.

Mr. STUPAK. Thank you. Thanks for letting me go over, Mr. Chairman.

Mr. UPTON. Mr. Burr.

Mr. BURR. To both the generals, do you both agree with what the Secretary just said about a decision at the labs to break out security separately and negotiate a new contract with the labs that would allow you to put a security entity in place to be in charge of security?

General Gioconda?

Mr. GIOCONDA. Sir, I am the staff officer that is assigned by the Secretary to come up with the range of recommendations.

Mr. BURR. Is this your recommendation?

Mr. GIOCONDA. The range of options to choose—yes, sir.

Mr. BURR. It is?

General Habiger, are you in agreement with it?

Mr. HABIGER. Sir, I will defer to see what General Gordon comes up with, sir.

Mr. BURR. I will take that as a very hesitant answer.

Mr. HABIGER. It is.

Mr. BURR. I appreciate it, then. I appreciate the honesty. Because I am sitting here as a member, and the last thing I want to

do is try to make some decision as to what the proper security is for Los Alamos or for Livermore or for Sandia. And for some of the people that come in here and testify, I feel like I have been there as many times as they have, once. And the last thing you need is input from me.

But we have had an opportunity over the last several years to see the problem in its totality. And one of the problems is the right and the left hand never see each other. One of the problems is that the line of communication—and I think Mr. Robinson said it very well in his testimony—just does not exist to the degree it has to for something as sensitive as national security. And for that reason, I am flustered, for the lack of a better word right now, to believe that we can just go out and renegotiate a contract, bring in a new entity, call this a security program and without fundamental changes in the line of communication, both with the labs, the new security company, walk away and feel good and believe that anything is different.

One of the problems I am convinced today, right or wrong, it was believed that there were areas that the labs weren't responsible or did not think they were responsible for as it related to special programs, because I can't believe that there wouldn't have been stricter things in place if they thought it was their decision. And I think they have expressed, through faxes and through conference calls, hesitancy with the deterioration of some of the security methods.

So it sounds great, Mr. Secretary, but I don't think it can work without a significant fundamental change to the operation, both on the labs' part and the security part. And if we can accomplish that, I am not yet convinced that they can't continue to supply the appropriate security, and we have eliminated another layer that might further blur the problem down the road. It is a personal observation, and I wait with some degree of anxiousness to watch how, in fact, this is structured.

Mr. Secretary, on March 1, 1999, these three directors had a conference call with Secretary Moniz, and they faxed to him a recommendation to reinstate the formal accountability. Do you know what happened to that recommendation?

Mr. GLAUTHIER. I am not clear exactly what happened. I understand that that was written up after a meeting at which some of those topics were discussed.

Mr. BURR. I believe it was a conference call between the three directors, am I correct, to any of the directors?

Mr. ROBINSON. That was my memory, yes.

Mr. GLAUTHIER. When I discussed it with the Under Secretary yesterday, he did not have a recollection of the specific memo and the like. It's clearly a topic that was discussed at some level, and it was at a time when security issues were very prominent last year, as you recall. The Secretary and the Department took a lot of action on various fronts. We had, as I indicated in the testimony, about 50 different security and counterintelligence measures that were implemented as a result of last year's event. So I think that this must have been a part of the overall pattern. But it came in just before I arrived and I am not sure exactly what happened to it.

Mr. BURR. Let me just read the last paragraph. I don't think I read it when I entered it into the record. And I assume that it got there, and maybe somebody can tell me whether it was acknowledged: "The directors of all three of the DOE nuclear weapons design laboratories are in agreement that the former controls should be reinstated as quickly as possible. This recommendation is presented to the Under Secretary and counterintelligence officials for their evaluation of what, if any, problems might result from prompt reinstatement of the previous policy."

Let me ask General Habiger—I think you have been there the longest—next. Did you have any recollection of this? Or was it ever mentioned to you?

Mr. HABIGER. No, sir. The first I was made aware of that was approximately 2 weeks ago.

Mr. BURR. I hope all of you can understand how that makes us feel as we try to wade through this. There were some pretty good signs from our lab directors, we do not think we are doing the right thing, that seem to not only have been discarded by the individuals that were given those, they can't even be uncovered now except for the process that we are going through. I know that we will have another round, and I thank the chairman and I yield back.

Mr. UPTON. Thank you.

Mr. Cox.

Mr. COX. Thank you. I just want to register—I'm sorry Mr. Stupak has left—my strong agreement with my colleague from Michigan. He is absolutely right. The Department of Energy used private security at foreign launches—the Department of Defense, I should say, used private security at foreign launches, and it was a failure. And one of the recommendations of Congress was to make sure that we take that responsibility on as the U.S. Government. The U.S. Government is responsible for the national security. It must not be privatized. And the notion that we are going to, because we necessarily use academics when we are trying to contract for science, that we are going to contract now additionally for security ought to be unacceptable on its face.

That is why Congress created the NNSA. Congress created the NNSA so that there would be a clear line of authority virtually independent of all the rest of the bureaucracy at the Department of Energy, and it would have exclusive responsibility at the national labs over intelligence and counterintelligence, for example.

But I am hearing here today another endorsement of blurred lines of authority, and I wonder whether you could, Mr. Glauthier, explain why it is that Congress should look favorably upon bringing in additional private contractors to be a new layer of authority in providing security direction for the national laboratories?

Mr. GLAUTHIER. Certainly, Congressman. First of all, we agree very much with the need for line accountability and for clearing up what has been, in many cases, a blurred sense of responsibility, of staff versus line responsibilities in the Department. We want very much to see the NNSA responsibility carried out very directly from Under Secretary Gordon to Defense Programs, to the field offices, to the laboratories, and have that accountability apply to missions and security and safety and all the other functions there.

Having said that, we also see in the past that the experience of the laboratories has not always been outstanding in some areas that are not the science areas. Science is clearly their forte. It is the strongest area. But security, construction management, some other things that are not as closely allied to the academic areas, for the University of California labs at least, have not been as outstanding. And it is those areas we are looking to try to strengthen. We might do it through a joint venture with the university and another firm. I have talked with the provost and the management of the university about different models. They feel very strongly that they ought to have some continued responsibility.

Mr. COX. What the laboratories are telling us is that they are creating the information—and I think we are misusing the term "responsibility" here, because—or at least we are using it in multiple senses. Obviously, lab employees, scientists and others, are responsible for the information they handle. They are responsible in that sense. But it should be equally obvious that every employee cannot be equally responsible for establishing the rules. And that ought to be the responsibility of someone who clearly has authority to implement those rules. And when the rules aren't followed, there ought to be clear accountability, which we have been lacking every time we have had an oversight hearing when something goes wrong.

And every group that has looked at this, the Select Committee that I chaired, was one in a long stream that extended earlier and went beyond that, all said the same thing. Everybody that has looked at this has said that the lines of authority are not clear, and that is why the Congress created the NNSA.

Now, earlier when we had a report from the Office of Independent Oversight and Performance Assurance, we heard from the head of that office that he does not know much about polygraphing; he does not know much about counterintelligence, and so on. The compartmentalization of this and the blurring of lines of authority is incongruous with the real world.

If you take now a private contractor and slide them in between the Department of Energy, the NNSA, the lab management, and so on, I cannot imagine how that does not make matters worse.

Obviously, they are going to be setting the rules—or are they not going to be setting the rules? What are they going to be doing?

Mr. GLAUTHIER. Their focus will largely be on implementation. They will set some of the specific practices for how to actually live up to the standards.

Mr. COX. So when they are setting specific practices, do the labs report to them?

Mr. GLAUTHIER. Well, I think, for example, what kind of a log should there be in the vault?

Mr. COX. Let me ask a more specific question. How does this private contractor relate to the NNSA? Does it work for the NNSA?

Mr. GLAUTHIER. Yes.

Mr. COX. All right. And does it work for the lab or above the lab?

Mr. GLAUTHIER. Well, that is part of what General Gordon is supposed to decide this summer with the university. Should it work directly for the NNSA in parallel with the University of California contract or——

Mr. COX. What is the advantage of not making these people employees of the U.S. Government and the NNSA? What is the advantage of having it be privatized?

Mr. GLAUTHIER. Well, they are it is already not employees of the Federal Government. They are now the University of California employees, in the case of those two laboratories.

Mr. COX. The function you are talking about creating does not presently exist. You are talking about going out presumably to the private sector and sliding it in. So it is not fair to say that presently it exists when it isn't created yet. The NNSA does not yet exist. Even though the Congress passed the law a year ago, the administration has so dragged its feet that we have had nothing. And of course, the politics in the Senate as well, the minority in the Senate held up the confirmation of the administrator, as you know. Now we are finally getting it off the ground and it is just a matter of weeks now. With the NNSA just now getting up and running, why would we not want to have the NNSA perform the functions that Congress just gave it in statute? Those very functions you are talking are about the statutory functions of the NNSA.

Mr. GLAUTHIER. And we do intend for the NNSA be responsible for carrying this out. The way they perform most of their functions is through contractors at the various facilities. So it will be natural for them to use a contractor in some mode. The question is in what mode? What's the right way? Should it be through the university or in parallel to it? Those are things I think they need to——

Mr. BURR. Will the gentleman from California yield for a clarification? Do you also envision that the field offices would be in charge of the evaluations for the security company as well, the DOE field offices?

Mr. GLAUTHIER. The field office, in their role as administering the contracts, would continue to do that. We have, as you saw this morning also, an Independent Office of Security Oversight headed by Glenn Podonsky. We would expect that office to also provide oversight and evaluation of these activities.

Mr. BURR. I thank the gentleman for yielding.

Mr. COX. Well, I think we are headed off in the forest here. I think it is going to get much worse if you do this.

Mr. UPTON. Ms. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman. I would like to pick up this same line of questioning here, and I am glad that there are some members of the DOE at this table who are skeptical about this proposed new arrangement, because I think it exacerbates the very problem that we are identifying here, and it sounds pretty dysfunctional to me.

I have to always put things in a little bit simpler terms, I am afraid. At our house we have some rules. You have to close the front door when you come in and out. You are supposed to keep the lid on the jug of milk. You are supposed to close the refrigerator door and push in your chair after you get up from the table. We repeat those rules. We try to be clear about those rules. We train to those rules. And there are consequences if you do not follow those rules.

But what I hear you saying with this new contract here is that you are going to bring somebody in and post the rules on the refrig-

erator, and then you are going to come in and check and see if people have done what they are supposed to do. But I am no longer in charge of training and controlling and repeating and consequences and all those things. That may be a little simple, but that is kind of the way I see this new security contractor.

And I wonder if perhaps, since I noticed, Paul, you referred to, in your testimony, the importance of integration, and since you are not the direct guy who is immediately affected by this possibility of a new contract, if this kind of thing were imposed on the other labs, would it work?

Mr. ROBINSON. I am worried about anything that splits the authority and responsibility. As I said in my written testimony, I believe the preferred direction is to try and streamline authority, responsibility, and accountability. Only if you do that do you have a chance of knowing who is responsible and being able to take action.

I also am a believer with a little bit of experience over time that when you have that clean line of responsibility, people, in fact, grow to deserve it instead of shrinking from it if the lines are blurred.

Mrs. WILSON. Thank you. I want to change the subject a little bit, because I have some questions about the NEST chain of command. And I wonder if maybe General McBroom, you are the person to ask this. Can you describe the chain of command for the NEST and who is responsible for what?

Mr. MCBROOM. There is normally—we pay for a couple of people in each site. The number varies. Most of them we pay them, I think, seven full-time salaries at Los Alamos, but that includes the secretary, and we have a small contingent there that works primarily on NEST operations, and then we will have another couple hundred people that do not. Normally, there is a designated point of contact at each site that we deal with from the staff that deals directly with the NEST team. So that chain of command would go from myself to my program manager at the staff, right down to that program manager at the site.

Mrs. WILSON. The University of California said in a letter on June 20, and Dr. Browne also mentioned it in his testimony, that line managers at labs had little or no access to ensure that lab safety and security rules are met for these close-hold programs. Is that—do you agree with that?

Mr. MCBROOM. I think that there was nothing preventing them from doing that. I think that there was some confusion at the site. I would go that far. But I mean, there is nothing—I went back to the—I have been there for 9 months now. I went back to the two previous directors and talked to both of them and they both said no, definitely we've never said that people can't look at it, that it shouldn't be looked at or anything like that.

Mrs. WILSON. But there was confusion as to who was responsible?

Mr. MCBROOM. I think there was some confusion there. I hope—I sent something out the first week of June moving the control to Albuquerque Operations. Because the operation, when I got there, was done with the headquarters deploying with the teams. And I thought that kind of confused the mission, the oversight mission

and the—and what we were really supposed to be doing at the headquarters.

Mrs. WILSON. General, when was the last time the Department of Energy did a program-wide security audit or assessment of the NEST program?

Mr. MCBROOM. I have no idea. I am a force employer. I am not a security person. That is a security question.

Mrs. WILSON. Who would be responsible within DOE? You talk about this is a team drawn from people from all over the country, all different responsibilities; they end up in some airport somewhere. Who within DOE is responsible for this whole thing?

Mr. MCBROOM. When they are on the road?

Mrs. WILSON. No—well, for the program. Who runs the program?

Mr. MCBROOM. I run the program. I am responsible for the team when they are on the road. When they leave that lab, I have operational control. I do not have administrative control. Administrative control, disciplinary action, firing, things like this, remains with the lab. Just like when they are on the road, they follow lab procedures. My people are out there to focus on the emergency and to help the scientists do their job.

At the same time, we look at security and safety just from a standpoint of doing the way the headquarters said we should do it.

Mrs. WILSON. Dr. Browne, did your folks feel as though they had the authority to do security audits of the NEST team?

Mr. BROWNE. Well, I think you hit one of the points that the General referred to about some concerns at our laboratory. Our program manager, who I am no longer allowed to talk to because of the FBI investigation, but what I can talk to you about is that he wore a couple of different hats. He wore a hat inside the laboratory where he reported to our management for organizing and coordinating the program inside the laboratory, and he also wore a hat for the Department where he was responsible for activities at Livermore and Sandia.

He made some comments to our security people that they were not allowed to look at the NEST operational security because that was his function. And my opinion is that there was a lack of formality of operations that would have clearly defined the roles and responsibilities of people at Los Alamos for this program. I think it's missing. You know, I'll share some of the blame for that. I think we should have caught that. But, in fact, I believe it was missing. There was no line manager that had his or her signature on that plan, the security plan.

Mrs. WILSON. One final question, Mr. Chairman, if I may. This memorandum from the lab directors concerning increasing level of security from March, I understand the Under Secretary has no recollection of receiving this. And I can understand that. All of us up here get about 5,000 letters a month. But in our office, we do have a process for identifying, by number, each incoming letter. Does the Under Secretary have a similar system?

Mr. GLAUTHIER. We do have that kind of tracking system, and my understanding yesterday, when I discussed this in our office, was that this was never actually submitted to us in the mail or in the normal transmittal system. It was faxed to his office and,

thereby, avoided the regular process. It wasn't captured in the regular tracking system.

Mrs. WILSON. Let me make sure I understand. The Under Secretary's correspondence management system, you have checked it and you can find no reference to this memo?

Mr. GLAUTHIER. That was what I was told yesterday, that's right.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. UPTON. Thank you. I want to go back to a question that was I focussing on when my time expired a little bit early.

Mr. Glauthier, who is the individual or the department that is actually responsible for the classification in terms of security with regard to the material at the labs?

Mr. GLAUTHIER. The classification responsibility?

Mr. UPTON. Who determines whether it is Secret or Top Secret?

Mr. GLAUTHIER. I think it is actually at the laboratories themselves, the people who develop the material. No?

Mr. UPTON. Dr. Tarter?

Mr. BROWNE. There is a classification guide that is developed by the Department that the laboratories provide technical input to.

Mr. GLAUTHIER. But the actual decision on a particular document using the guide I thought was actually done at the lab. The guide itself is developed by the Security Office.

Mr. UPTON. So who would have been responsible? For example, these hard disks—the hard drives that were missing, who actually determined that it was Secret versus Top Secret?

Mr. HABIGER. We have——

Mr. UPTON. Whose chain of command?

Mr. HABIGER. Chain of command would go from the program office to the laboratory. I have a group of people, who are subject matter experts, develop classification guides. Those guides are then sent to the field offices, the laboratories, and the program offices.

Mr. UPTON. So are you saying are the directors—ultimately, as they are in charge of the security of the entire lab site, are the three lab directors, these particular NEST tapes that the NEST team lost, is it—was it Dr. Browne's responsibility that they were Secret versus Top Secret?

Mr. HABIGER. It would be classifiers at the laboratory.

Mr. UPTON. Who did they report to? I mean, ultimately to Dr. Browne and up, or did they go back to General McBroom or who?

Mr. BROWNE. Mr. Chairman, let's see if I can explain this. Each piece of information on the hard drive by itself was secret RD and would have been classified as such if it were a piece of paper or on an electronic medium.

Mr. UPTON. Right.

Mr. BROWNE. The compendium, I think, is the issue here, the large amount of information. There was no guidance in existence about how we treat large encyclopedic data bases at a higher level.

I would like to mention that I just found out, after I read—after I wrote my testimony, that we did submit in September 1999 to the Department a letter requesting that these hard drives be encrypted. One of the difficulties is that the software for encrypting information, until recently, and I believe General Habiger can point out in more specificity, that it did not exist. So even though we

made a request in September, it was not possible to accommodate it.

Mr. UPTON. Although I am told that, at least at Livermore, some portions of the hard drives have, in fact, been encrypted and at least for a number of months, is that not true?

Mr. TARTER. What we did, we used a nonNSA-approved encryption technique because, as Dr. Browne said, there was not an NSA-approved encryption. It was our decision that—we call it—some encryption was better than no encryption.

Mr. UPTON. Did you share that information with the other labs, or did the NEST teams—was it actually a part of the NEST team that did that?

Mr. TARTER. It was part of the NEST team that did that.

Mr. UPTON. And did they not share that information with the NEST teams at the other two sites?

Mr. TARTER. They did, and I have the—you know, we can go into more detail if you wish. I have the head of the NEST team here. I think we had those discussions, and I think in the absence of an official NEST policy and since ours was not approved in the NSA sense, I think it became local option.

Mr. UPTON. General McBroom, were you aware of that at all?

Mr. MCBROOM. No, sir.

Mr. UPTON. So you have really wiped your hands clean altogether of the security at the site of the material, is that right? Your role is really just the operations; the phone rings and then out the door and then you have them under charge; is that right?

Mr. MCBROOM. Yes, sir. I am the force employer. They provide a head, two arms, two legs, and a 20-pound brain with a piece of equipment. I employ those people out there. I watch to make sure, while they are in my charge, what they do when they are at that site, but primarily they still come under those rules.

Mr. UPTON. Dr. Tarter, your answer again as to whether that information was shared between the three teams, it just wasn't done; or was it?

Mr. TARTER. We did—we had those discussions with Los Alamos. We said what we were going to do, and I think they chose, in the absence of either an approved status for the encryption technique we were using or formal guidance, to continue with the local option.

Mr. UPTON. Did you talk to DOE about what you were doing? Was DOE aware?

Mr. TARTER. Apparently yes. Again, if you wish, you could swear in the head of our NEST team for a more precise——

Mr. UPTON. We might just do that. Just get that—is that individual here, behind you?

Mr. TARTER. He retired a week ago but, yes, he is here.

Mr. UPTON. Just come up and identify yourself for the record.

Mr. TARTER. This is Dr. Alan Mode.

Mr. UPTON. Just remain standing there for just a second.

[Witness sworn.]

Mr. UPTON. You are now under oath.

If you would just describe the set of circumstances behind this. I know my time has expired, and I will yield to Mr. Stupak.

Mr. MODE. It is, as Dr. Tarter has described, the request and information had been discussed within the NEST community. There was not an approved encryption technique available at the time. DOE had made that request some time ago for an approval from—NSA-approved encryption technique. It was purely a local option. We—our people just felt a little more comfortable. We also recognized that it was not an approved encryption technique, and in one sense you could argue that we were, in fact, acting outside of our bounds by imposing an encryption technique that had not been approved.

We encrypted the Livermore portions of the information. We did not encrypt the Los Alamos portions. Again, with their knowledge and——

Mr. UPTON. How long did it take to encrypt the information?

Mr. MODE. I am sorry. I don't know. We used—in open hearing, I won't say exactly how we did it, but not an extended period of time.

Mr. HABIGER. Mr. Chairman, if I could point out that NSA, National Security Agency, certified encryption on June 19 and we were the first ones in the government to buy it.

Mr. UPTON. Right. I understand that, but I think this actually took place—nonNSA-approved happened, what, September last year, thereabout?

Mr. MODE. Approximately January 1999.

Mr. UPTON. January 1999?

Mr. MODE. Yes.

Mr. UPTON. So literally a year and a half it took.

Okay. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

Dr. Browne, you said something that bugs me a little bit. You said that you are responsible for the information that would go on the hard drive that—whatever segment it is—and there are many Top Secret segments on this hard drive.

Mr. BROWNE. Secret. Secret RD.

Mr. STUPAK. Okay. Secret?

Mr. BROWNE. Correct.

Mr. STUPAK. So in, say, year one, there might be a thousand pieces of Secret on that hard drive?

Mr. BROWNE. It is less than that, but let's say many.

Mr. STUPAK. But then you said you weren't responsible for the encyclopedia of the information on it there.

Mr. BROWNE. No. I said there is no DOE guidance that tells anyone that once you have accumulated any amount of information, that you should classify it at a higher level.

Mr. STUPAK. But do you really need a guideline to figure this out?

Mr. BROWNE. We don't have the authority——

Mr. STUPAK. I mean, if you have one piece of information that's so important, now you have all kinds of pieces on there, I think that hard drive just becomes more valuable. I don't think I need a government guideline to tell me not to drop it behind the copier.

Mr. BROWNE. Well, I don't disagree with that, but we don't have the authority to classify something Top Secret or not.

Mr. STUPAK. But you have the authority to provide security and control——

Mr. BROWNE. Correct.

Mr. STUPAK. [continuing] for this?

Mr. BROWNE. Absolutely.

Mr. STUPAK. Because I guess my concern—and is it your testimony that you did not believe you were responsible for security over the NEST team and the information under their control?

Mr. BROWNE. No. I believed I was. My comment was that our security people were told by our NEST program manager that they did not have the right to come in and look at the NEST program operations; that it was a closely held need-to-know program. A limited number of people had access to that program and access lists, and so they were—they were told that they were not to look at this program.

Mr. STUPAK. Who do the security people work for?

Mr. BROWNE. They work for me. They did not bring that to my attention.

Mr. STUPAK. So even the people under your control who are doing security, plus your scientists, they don't agree who can look at what and who has control over what?

Mr. BROWNE. That's an issue, and I brought that up with them since I found out about this.

Mr. STUPAK. So now the proposal is to put another entity out here, yet to be hired, to even have more arguments on who is controlling and who has the authority?

Mr. BROWNE. No. General Gioconda sent me a very excellent letter, I believe it was June 16, saying if there is any confusion about any program, you have the authority to investigate it unless you are directed not to investigate it.

I have used that letter now to look into a series of programs that are very similar to NEST.

Mr. STUPAK. When did you get that letter? Maybe I was out of the room and I had to make a phone call.

Mr. GIOCONDA. I happen to have a copy.

[The information referred to follows:]

Department of Energy
Washington, DC 20585

June 16, 2000

EXPEDITE

Memorandum for the Managers, Albuquerque and Oakland Operations Offices

From : BGEN THOMAS GIOCONDA
Acting Deputy Adminstrator for Defense Programs

Subject: Laboratory Responsibility for Security Oversight

This memorandum is to reconfirm the responsibility of the nation's nuclear weapons laboratories for assuring that proper security procedures are followed in ALL activities performed on laboratory property or under laboratory auspices. No program can be exempt from such oversight without written approval from me or my superiors.

cc:

Director, Lawrence Livermore National Laboratory
Director, Los Alamos National Laboratory
Director, Sandia National Laboratory

Mr. STUPAK. How long ago—when was that written?

Mr. GIOCONDA. Well, sir, I sent that letter on June 16 because I was surprised, too. John brought it to my attention. Let me read it to you.

Mr. STUPAK. Okay.

Mr. GIOCONDA. It says, "This memorandum is to reconfirm the responsibility of the Nation's nuclear weapons laboratories for assuring that proper security procedures are followed in ALL"—all capitalized—"activities performed on laboratory property or under laboratory auspices. No program can be exempt from such oversight without written approval from me or my superiors."

Mr. STUPAK. That was because labs were saying that they didn't have responsibility here?

Mr. GIOCONDA. They were—as Dr. Browne described, apparently the program manager said stay away from my program. No, he did not have the authority to do that.

Mr. STUPAK. Well, this is really sort of the same argument that we have been hearing since about 1976 when Mr. Dingell first brought this to our attention. And if you go through this, this responsibility, this lack of accountability, we have had these concerns brought up in 1976, 1982, 1988, 1992, 1997, 1998, 1999 and now again in 2000. We always get these assurances things will be different. Now we have a letter saying they have to be different, but they never really are. And I guess that's the frustration we see on this side of the dais.

Mr. GLAUTHIER. Congressman, may I comment?

Mr. STUPAK. Sure.

Mr. GLAUTHIER. One of the changes that Secretary Richardson made in April of last year was a reorganization to make explicit staff versus line responsibilities, and at that time we actually had

discovered that the head of Defense Programs claimed he had no responsibility for security; it was somebody else's responsibility.

We made it very clear that that responsibility is a line responsibility, and implementation and accountability for security flows right through the whole organization, but that has been a problem over the years.

Mr. STUPAK. Sure, but that was last year. And now it seems like we don't get this thing really cleared up now until this June 16 letter here from the General.

Mr. GLAUTHIER. I think what you are hearing is one specific area. These NEST programs were a point of confusion at one of the laboratories. I believe, you know, the vast majority of the people understood the responsibility was in fact much clearer, and this was just to clear that one piece up.

Mr. STUPAK. But it really should be clear that the NEST program manager is a lab employee, right?

Mr. GLAUTHIER. Absolutely.

Mr. STUPAK. I was really interested, Dr. Tarter, you mentioned your own little local option that you put on the hard drives, the encryption?

Mr. TARTER. Yes.

Mr. STUPAK. That's just something that you thought was necessary?

Mr. TARTER. It seemed good practice.

Mr. STUPAK. And security is part of your responsibility, right?

Mr. TARTER. Right.

Mr. STUPAK. Thanks.

Mr. UPTON. Mr. Burr.

Mr. BURR. We have spent a lot of time on the 3-1-99 fax, whether it came or didn't come. Let me just share with you, Mr. Secretary, and this is out of the Redmond report: "Comprehensive classified document control system—document controls for the most sensitive data of the weapons lab should be reinstituted by the agency director. The program should be constantly monitored by a centralized agency authority to ensure compliance"—basically what the three directors said.

So if you didn't get it in March, in June you certainly got the same message from Senator Rudman; and still today, a year later, we don't have that policy back in place, or if we do it's a recent one.

And, General Gioconda, I want to commend you for recognizing there might have been a lack of communication on the labs' understanding of their jurisdiction and where it did or did not stop, and your quick response to get a memo out that says, no, here is where it extends to; because I think that's the type of thing we have got to clear up, some of the misunderstandings that exist, if we are going to move forward at all, and I think that the directors, though they may not always be in agreement, I think they are appreciative of clarification.

Mr. GIOCONDA. Sir, I have only been in an acting capacity since August of 1999. I am a history major, so I went back and read all of the history that you have read. It really boils down to—and I just want to say—because I got the impression that when I gave you a "yes sir," that I am supportive of the decision to go and look

at options and how to make this situation better, that somehow was a problem. I would wait until you see what Under Secretary Gordon comes out with on 5 September, regarding negotiations with the University of California before you make your judgment about whether this can work, because this decision will be made within the NNSA process.

General Gordon is my boss. I am the Acting Deputy Administrator to him for Defense Programs.

But it really boils down to four things. When I took over and told everybody here at the table that it is, one, you have to stay focused on the mission, and we have to be very clear to do that. Really, the mission is safe, secure, and reliable nuclear weapons. It isn't harder than that. And if we do anything to damage that, I am concerned about any security, any arrangement we have. That's important.

Mr. BURR. So you feel confident—I may not be here and you may not be here, but there will be someone on this subcommittee, if it doesn't work, who asks the question why did they do this and why didn't they have more vision than that?

Mr. GIOCONDA. Yes, sir.

Mr. BURR. I am not prejudging it. I am raising what I think are legitimate questions but, more importantly, legitimate concerns based upon my interpretation of the history that I have read and certainly what I have seen firsthand for the last 5½ years since I have been here as it relates to the relationship between the agency and these labs.

Mr. GIOCONDA. Sir, if I may, two more things.

Mr. BURR. You may.

Mr. GIOCONDA. Accountability and responsibility has to be in this environment. I agree with you, as the staff officer that's going to put some of the ideas together, that if you remove accountability and responsibility from individual scientists who create a lot of this data, this won't work.

And then the third thing I will tell you is the chain of command. The chain of command has to be followed in this organization, and that's a lot of what happened back in April when they made sure that the line is involved.

That's why I am at this table. I am responsible for this incident. Defense Programs is responsible down to the weakest link in its program. We have got to get that across to everybody in Defense Programs, and if you walk around the complex, sir, as I know you have, 99 percent of them know that.

Mr. BURR. Well, one of the questions that I had earlier was from—and I can't lay my fingers on it right now, but it was basically the fact that many of the Secretary's initiatives of late, this last round, were not decisions that were based upon conversations with the directors of the labs. And it may have come from Mr. Robinson's testimony, that this was a—this was a somebody makes the rules and somebody else lives by them. This is not a shared process of adults that get together to try to figure out how to make it work the most effectively and the most securely that we can. And I would tell you, that's an important part of the process and any criticism of how we reach that, I would hope that you and others would take it hard and that we would find inclusion in the process.

I have just a couple of—I know my time is already out, but I have to finish this before I go because I have got a meeting.

Let me just ask one of the directors, do all scientists sign a commitment to take a polygraph if the need ever arises?

Mr. ROBINSON. They do not.

Mr. BURR. They do not. But my understanding, and correct me if I am wrong, NEST members have signed an agreement for a polygraph, if needed?

Mr. ROBINSON. They have not.

Mr. TARTER. No, they have not.

Mr. MODE. No.

Mr. ROBINSON. What is the case—and let me first go to non-DOE programs where polygraphs have been employed for a decade. If a scientist were going to be assigned to that compartment, they had to then agree to take a polygraph or they could not go into the information in that compartment, but it is not a general thing throughout the laboratory. So it is program-specific, compartment-specific for polygraphs.

Over the course at our laboratory, about 220 people were polygraphed as a part of those programs.

Under DOE programs, we identified just above 200 people who are members of the compartments that were just made—that polygraphs were just made mandatory. Taking some of the people who had been polygraphed within the previous 5 years, so you didn't have to do them again, our number came down to 171 people. We have polygraphed 46 of those as of a week ago, so I suspect the number is well above 56 at the present time.

Some of the members of our NEST team, when faced with the question of a polygraph to continue as members of NEST, chose to opt out and resign from this responsibility.

Mr. BURR. So it is not a requirement of NEST now?

Mr. ROBINSON. It is a requirement now.

Mr. BROWNE. I don't think so.

Mr. TARTER. No.

Mr. ROBINSON. No?

Mr. BURR. Just to express my own frustration, somewhere in—since the latest problem at Los Alamos, somewhere in the conversations, whether it is with labs or whether it is with DOE, I was led to believe that it was standard protocol that every member of the NEST team signed a waiver that said I will be polygraphed if you ever need it. So we can even be mistaken up here, based upon the information that we hear.

I hope that if there is a policy on that, somebody would let us know.

Mr. ROBINSON. I have got a clarification from my own folks. Those who are in certain roles within the program have to be, but not all members of NEST have to be polygraphed if they are a part of what is called the PSAP program, Personal Security Assurance Program.

Mr. BURR. I would say to Mr. Aftergood, if those people have signed a pre-waiver on a polygraph, I would not expect to see them with a badge on in the facility saying no polygraphs.

And you are right, they do have a right to. They also have a choice of where they work.

One last thing, Mr. Robinson. You said in your testimony—and if this is not something we can get into, then certainly feel free to tell me, we will follow up in another way. In your testimony it said, talking about controls on electronic media, said the other issue—talking about two things that you have found as you have gone back and looked at your system—reported on June 30 involved a single 3½ inch 1.44 megabyte disk that had not been yet located. Inquiry is currently underway in accordance with DOE's procedures.

Is that still the case? Have we still got something that's missing?

Mr. ROBINSON. It is unaccounted for at the present time.

Mr. BURR. And is that of a nature that we should be concerned?

Mr. ROBINSON. It is always a concern if you have anything that's a secret item that is accountable.

I might point out that only because that work group, which is our largest holder of classified information in the weapons engineering department, never took off the accountability system for Secret or Top Secret information, that we in fact know that it is missing; but the content of what is on the disk we know, and it is not of the same magnitude as other things. It is very high-level information. There is no detailed information. There are no figures.

Mr. BURR. Well, we are relieved with that. And just for the purposes of my colleagues, I want to point out two things in Mr. Browne's testimony. The first one was, "since 1994 we have had 19 DOE inspections that cover vault operations. These resulted in two findings." One finding that's closed, involving a technical issue regarding alarm testing, and has corrective action. Neither of the two findings address the issues surrounding this incident.

And later on in—or earlier in your testimony, I would like to point out, "the laboratory security programs were reviewed 16 times in 1999 alone."

I say this for the purpose of everybody here. This is not a question of whether we have investigated, whether we have had enough inspections. I truly think that if we asked Mr. Podonsky to go back six more times to every facility, he would very politely do it. He would come in with a very detailed analysis.

Folks, until we all care, until we decide that we are going to make the fundamental changes that have to be made and that I believe the people that we have got in place are capable and willing to make, we are not going to solve the problem. No matter what we come up with in the way of new inspections, no matter what we come up with in breaking the security entity out separately, if you are not willing to make the structural changes and to require the accountability, then you have got to be prepared to keep coming back to this subcommittee.

Mr. Chairman, I yield back.

Mr. UPTON. Thank you.

Mr. Cox.

Mr. COX. Thank you. Mr. Glauthier, earlier, not in this round but in the previous round, Mr. Burr asked a question. And then perhaps Mr. Burr can help me. Mr. Burr, as you leave, you and Mr. Glauthier had an exchange about the field offices and the relationship potentially to these new privatized security people we are

thinking about hiring. Do you remember what your question was and what the answer was?

Mr. BURR. My question was, did the Secretary envision that the field offices would be in charge of the evaluations of this new security entity, just like they are currently responsible for the evaluation of the contractors of the labs, both for their administrative and their security performance?

Mr. COX. And my recollection, Mr. Glauthier, is that you answered yes.

Mr. GLAUTHIER. Yes, that's right.

Mr. COX. Now, I don't know whether you have read the House Armed Services Committee Report dated February 2000 on the proposed DOE implementation plan of Title 32?

Mr. GLAUTHIER. No.

Mr. COX. Which sharply criticizes the maintenance of pre-Title 32 reporting relationships and specifically focuses on the role that the field offices have played.

Let me just read a portion of it. "The panel notes with concern that the plan"—this is the Department of Energy's plan—"explicitly sustains current reporting relationships between the NNSA contractors"—and these new contractors would fall, of course, into this category—"field offices, and headquarters staff. Thus, NNSA contractors will report to the Deputy Administrator for Defense Programs through the field offices rather than directly to the Deputy Administrator. Several studies have found that this arrangement has generated redundant and confusing lines of authority in the past. Despite strong criticism in the President's Foreign Intelligence Advisory Board and other reports, no changes in the field office reporting structure are contemplated. Furthermore, section 3214 of Title 32 states"—that's the law—"that the NNSA facility should report to the Deputy Administrator."

Now I have just read while we were sitting here, the whole Title 32 again to make sure I understood the law. Why is it that you are violating the law?

Mr. GLAUTHIER. My recollection of the law, I don't have it in front of me, is that it permits us to use a field structure in the line organization if we wish.

Mr. COX. Is the field structure part of the NNSA?

Mr. GLAUTHIER. Yes.

Mr. COX. Are the people who work in the field offices NNSA employees and not employees of the Department of Energy?

Mr. GLAUTHIER. They are both. NNSA is a part of the Department of Energy.

Mr. COX. Are they people who are hired exclusively by the Administrator of NNSA?

Mr. GLAUTHIER. It depends on the field office. The Albuquerque——

Mr. COX. Well, no, the law doesn't say that. The law says that except for certain named positions in the statute, it is the role of the Administrator to hire and fire people within the Administration, and furthermore the Administrator is given the statutory authority to set policies within the NNSA that are different from the policies and procedures in the Department of Energy, and only the Secretary of Energy himself can reverse those.

Mr. GLAUTHIER. Or the Deputy Secretary, if he is given that responsibility by the Secretary; that's correct. And in fact, the Secretary has the authority under the law to set policies that will apply to the NNSA as well.

Mr. COX. So why are we using these structures from the old system before the creation of NNSA?

Mr. GLAUTHIER. The field offices are part of a line organization, and that's where the contracting is done. They have processing of vouchers.

Mr. COX. I know that's how it used to work, but what about the new statute?

Mr. GLAUTHIER. The new statute doesn't require that we change that. It is up to the NNSA administrator, as you indicate, how that structure is going to be carried out and the implementation plans——

Mr. COX. Well, now, General Gioconda used to be an employee of the Department of Energy and now is a—is that correct, General?

Mr. GIOCONDA. I am not the best example to use, sir. I am a detailee from DOD to DOE.

Mr. COX. But you had a DOE function before?

Mr. GIOCONDA. Yes, sir.

Mr. COX. Now you have an NNSA function?

Mr. GIOCONDA. Yes, sir.

Mr. COX. So your relationship to the Department of Energy is semiautonomous.

Mr. GIOCONDA. Yes.

Mr. COX. In other words, the authority of the people who work at the Department of Energy over you can be exercised only through the Secretary himself or, if the Secretary is incapacitated or otherwise unavailable, by other statutory authority through his deputy, but acting qua Secretary because the statute is very explicit about that, and not in any other way. Is it your understanding that the same can be said for every employee in, say, the Albuquerque field office?

Mr. GIOCONDA. Sir, in Albuquerque they are all in the NNSA. That is clear.

Mr. COX. And then the DOE exercises no authority over that field office?

Mr. GIOCONDA. No, sir. The business functions are connected to DOE. They do have authority over the business functions that are connected to DOE.

Mr. COX. That sounds awfully confusing. Which is which? How do we know?

Mr. GLAUTHIER. May I? Congressman, may I respond?

Mr. COX. Well, the——

Mr. GLAUTHIER. The policies——

Mr. COX. I just want to remind you why I am concerned about this, because in questioning an earlier panel I read this portion of the report of 2 weeks ago from the Redmond panel, chaired by the former head of counterintelligence at the Central Intelligence Agency.

He said the DOE operational field offices at Albuquerque and Oakland continue to refuse to share relevant information from em-

ployee personnel files under their control with DOE CI, counterintelligence, or laboratory counterintelligence components. The Department of Energy counterintelligence is not even informed by these three offices when an employee loses his or her security clearance.

That's a mess.

Now, if NNSA is in charge of these people, then I want to call NNSA on the carpet for this performance. If DOE is responsible, then I want to call DOE on the carpet for this performance.

But the truth is, as we sit here in this hearing we don't know. Whose responsibility is it? Whose responsibility is that failure, NNSA or DOE?

Mr. HABIGER. Mr. Cox, if I may, sir, that is very dated information and is no longer applicable.

Mr. COX. Well, it is 2 weeks old.

Mr. HABIGER. Well, the report may be 2 weeks old, sir, but the assertions have been corrected some time ago.

Mr. COX. Were those assertions relevant to a time period prior to the enactment of Title 32?

Mr. GLAUTHIER. Before the implementation of it.

Mr. COX. Well, I understand you didn't obey the law for a very long time. And I am quite serious about this, because starting with the President of the United States own signing statement, there was a direct effort, documented by the Congressional Research Service, to subvert the statute. But I wonder whether or not this situation—independent of who shot John in this circumstance—obviously nobody is willing to own up to responsibility for this. But let me ask this question: Who is responsible for any defalcation today at the field offices? Would it be DOE? Would it be NNSA? Or is the answer, it depends?

Mr. GLAUTHIER. If it is a practice that they should be carrying out, the policy is in place and they are not doing what they are supposed to be doing, there is an NNSA responsibility; their line accountability to NNSA. On the specific information sharing of those personnel files, I would be willing to go back and get the specifics. I don't have those at this point.

[The information referred to was not received at time of printing.]

Mr. COX. Is there any aspect of the performance of the field offices for which DOE is responsible and not NNSA?

Mr. GLAUTHIER. Only in establishing some of the policies. There may be Department-wide policies on procurement, for example, that are issued to the NNSA and then implemented through the NNSA.

Mr. COX. Obviously that's not how the statute is supposed to work. The NNSA has ample authority to do its own procurement.

Mr. GLAUTHIER. But the statute also provides for the Secretary to determine policies that would be applicable to the NNSA.

Mr. COX. Well, I think the answer, plainly, which you have just given, is it depends on whether it is one or another kind of function at that field office. And sometimes presumably the very same people working in the Albuquerque or Oakland field offices we are describing here would be responsible to headquarters DOE, and other times they would be responsible to the NNSA. And what we are

now talking about doing is sliding in a new contractor that will have the same questions about who it reports to, because it is going to be reporting to somehow this field office which is itself a hybrid of DOE and NNSA, exactly what the statute was meant to prevent.

I think if I were out at the labs, I would not know who in the hell I am supposed to report to, and this is making it worse, not better.

Mr. GLAUTHIER. One point we are clear on is no one in the NNSA can take direction from people who are not in NNSA. We do understand that and have tried to implement it that way.

Mr. COX. Well, I think the chairman is being—perhaps I have more time. Do I have time further?

Mr. UPTON. I stopped the clock. If you want to ask another question, you may.

Mr. COX. The chairman is being generous. I do hope that we will recognize that there is a Presidential election in a few months, that whether it is a Gore administration or a Bush administration, if past transitions are any guide, most of the people in the Presidential appointment positions, not for terms of years, will be changed and so this ought not to be viewed as a turf battle. It shouldn't be about somebody in Congress taking away my power. We are not trying to take away the power of any individuals.

This is not a threat to Bill Richardson. This is a question about whether or not there can be an independent agency with only rare reporting relationships through the Secretary himself in charge of this function. And this administration, the Clinton-Gore administration, has fought it every step of the way, and I think it is doing a great disservice to our national security.

Mr. UPTON. Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman.

I am going to ask one open question and would ask anybody to answer it as truthfully as possible. Can this Member of Congress assure his constituency, or, more important, assure his children that the security and the problems we have articulated here in this hearing, both structural and institutional, will be corrected before January of next year?

Will the next administration have to solve this problem or will we have it corrected before January 1? Is anybody here willing to say that we think we will have it all taken care of by January 1; it will be wrapped up?

Mr. GLAUTHIER. I will be the first one to try to respond to you. I simply can't give an absolute answer, I think, to anything. One of our experiences over the years has been that that has always been a mistake. We are working our hardest to try to deal with the institutional and structural issues, as you have put it, and our hope is to have those in place, to have the NNSA elements in implementation, and then to have the continuing problem of, of course, the human element being something we always will have to deal with. But our hope is to be as far along that path as possible.

Mr. BILBRAY. Well, Mr. Chairman, I just want to say in closing that I grew up in a family where my father was a damage control officer who was at Bikini, at Eniwetok, who studied nuclear arms—was involved in the nuclear arms development in a peripheral

manner as a warrant officer. And I darn well believe that we all have a responsibility to make sure that his grandchildren do not have the technology he helped develop turned against those children, and I certainly hope that we can take care of this before we expect a new administration will have to take care of the problems of the past.

I yield back, Mr. Chairman.

Mr. UPTON. Mrs. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman.

Just to follow-up on what Congressman Burr was talking about a little bit, and what I asked as well about this issue of the facts. I don't want to belabor the point too much, but as you well know, representing Albuquerque, New Mexico, we have quite a bit of correspondence with the Department of Energy. And I asked my staff to go back and check, and everything that we send, whether by letter or by snail mail or by fax, gets a registration number and that registration number comes back as a reference on the reply.

And so without being too difficult about this at first, I would ask the chairman if he would request from the Department of Energy, copies of records of all items entered into DOE correspondence management systems for the week surrounding March 1, 1999, and also for a record of the fax receipts for March 1, 1999, for what I believe is Under Secretary Moniz's fax number, which is 586-7210.

Mr. UPTON. Without objection, Mr. Glauthier, if you can provide that for us?

Mr. GLAUTHIER. Yes, we will be happy to provide it. Normally, this would be logged in, so you are correct to expect that the system should have captured it.

[The information referred to was not received at time of printing.]

Mrs. WILSON. Dr. Robinson, there are some statements in your testimony which I found very interesting in light of your 32-year perspective of security. You talk a little bit about changes to the classification system that introduced systemic weaknesses in DOE's security system. I wonder if you could elaborate on that a little bit.

Mr. ROBINSON. I wonder if you would let me have 1 minute to comment on the question of the fax. In addition to the lab directors expressing our views in March of last year, as I say on page 9 in my testimony, I twice brought up in congressional testimony, once to this committee, exactly the same content that is the conclusion of this fax. So it has been something that has been a botherment to not only the three of us but to most of the folks who work in the laboratories; that all of this material, Secret, Restricted data as well as Top Secret, must be accountable.

The classification has taken on some serious problems in the decade of the 1990's. There was an order to declassify a larger amount of material and to speed up the declassification. In particular, within the Department of Defense, a lot of documents were declassified by category rather than someone looking at the document to see if there are paragraphs within the document that should not be released.

Unfortunately, in that process, some things went into the open that should not have gone into the open; and when we learned of it, we have been trying to pull it back.

The one unique thing about Restricted data, the Atomic Energy Commission controlled information, is it never has a time line associated with it, that it's declassified after X years, as is the practice in Department of Defense and most other parts of the government, Department of State, et cetera.

If the information could lead to the building of a nuclear weapon, as Mr. Bilbray suggests, to threaten our children, we would like to keep that information as bottled up as we possibly can in perpetuity.

So I considered it a fairly serious breach in the 1990's of declassification that led to some information going out.

I believe that was not the intent of the people who did the higher fences initiative. It was to still keep anything that could make a functioning nuclear weapon more possible to keep it classified, to keep it restricted from distribution.

Mr. COX. Would the gentlewoman yield for just a moment for a point of clarification?

Dr. Robinson, I think I understood you to say that the material at the labs is classified under the Atomic Energy Act.

Mr. ROBINSON. Correct.

Mr. COX. Is it the case that it is never classified under the Executive Order 12958?

Mr. ROBINSON. No. Some of the information in other programs than nuclear weapons that we work on and contribute to fall under that Executive Order and we carry out and use the stamps of declassify after 12 years, declassify after 25 years; but not information that could lead to a functioning nuclear weapon.

Mrs. WILSON. With respect to that, I understand that the lab directors resisted a lot of the changes that happened in the 1990's with respect to security and material control and so on. Were you ever told by the Department of Energy that if you didn't reduce your security controls you wouldn't be compensated for the cost?

Mr. ROBINSON. There is such a statement from the Albuquerque Operations Office, that this would not be cost reimbursable. I must tell you it was at that point not an issue of whether we were reimbursed or not. It is a question of national security.

Mrs. WILSON. So as a contractor, in this case not University of California but I would assume either AT&T or Lockheed Martin, you were told that you couldn't have a higher standard anymore; is that right? Or if you had a higher standard, it would come out of the hide of the contractor?

Mr. UPTON. Can I inquire about the date of that?

Mr. ROBINSON. I am quoting from a memorandum of June 19, 2000—whoops. Is this an attachment to it?

Oh, the attachment is June 29, 1992, and it says—the question is: May sites continue to account for all secret documents on a voluntary basis?

And the answer given by the Department was: Sites may continue to account for documents that do not require accountability under paragraph 2 but it must be at no cost to DOE. Costs associated with document accountability will be calculated only for documents that must be accounted for.

Mrs. WILSON. Mr. Chairman, I would like to ask if we could add that document to the record, if possible?

Mr. ROBINSON. Sure.
Mr. UPTON. Yes.
[The information referred to follows:]

United States Government — Department of Energy

memorandum

Albuquerque Operations Office
Kirtland Area Office

DATE: JUN 2 9 1992

REPLY TO ATTN OF: KAO:AR:SKI

SUBJECT: Accountability Requirements for Secret Documents

TO: J. D. Martin, 7400, SKL, Albuquerque

Reference is made to the attached May 15, 1992 HQ memorandum, same subject.

We apologize for the delay in retransmitting this memorandum, but the Albuquerque Field Office (AL) felt it was essential to delay action on the new policy until they were able to clarify several issues during the recent Information Security Working Group meeting held at HQ.

Attached to the memorandum is a question and answer paper, wherein AL has described the actions that must be taken to implement the new policy. They have also attempted to anticipate some of your concerns and address them in that attachment. There are probably some that they have overlooked and we will address those on a case-by-case basis either by telephone or memorandum.

If you have any questions or need additional information, please contact Stacy Ingram at 845-5416.

Brenda J. Marmeson
Chief, Administrative Branch
Kirtland Area Office

Attachment

cc w/attachment:
M. Lucero, 7442, SKL, Albuquerque

Modified Accountability Procedures

1. **Why are procedures for accounting for Secret documents being changed?**

   Two reasons are responsible for promoting the change: First, DOE must begin to prepare for implementation of the National Industrial Security Program, which will standardize security requirements among all Federal agencies. Second, administrative controls have proven to have little value added to security in a high-tech environment that uses computers, facsimile machines, and copiers. The accountability system will be replaced with more stringent physical controls and individual responsibility.

2. **What documents may be removed from accountability?**

   All Secret documents, including Restricted Data - Weapon Data, may be removed from accountability unless national requirements, agreements, or special programmatic needs mandate that the documents must be accounted for. Some examples are Communications Security keying material, North Atlantic Treaty Organization or Foreign Government documents, National Security Council documents, Special Access Program documents, etc.

3. **How is approval obtained to remove documents from accountability?**

   In order to obtain approval to implement the new procedures, organizations must submit a certification of inventory completion and reconciliation in the eleven point format contained in the May 6, 1991 HQ memorandum, "Modified Accountability Requirements for Secret Non-Weapon Data Matter." Additionally, security plans must be revised to reflect changes in protective procedures and training must be conducted to ensure that all personnel who have been granted access to classified matter are aware of your new procedures. Approval for removing matter from accountability has been delegated to the Field Office. Classified matter protection programs that have serious deficiencies noted during inspections and surveys will not be approved until the deficiencies are corrected.

4. **May documents in the possession of contractors or subcontractors be removed from accountability?**

   Yes, provided they are located in Limited or Exclusion Areas.

5. **May sites continue to account for all Secret documents on a voluntary basis?**

   Sites may continue to account for documents that do not require accountability under paragraph 2, but it must be at no cost to DOE. Costs associated with document accountability will be calculated only for documents that must be accounted for.

6. **Is a Document Control Station still required?**

   A central document control station is still required for sending and receiving classified documents. Substations are not required unless they are needed to maintain accountability for documents mentioned in paragraph 2.

7. **Are receipts still required for Secret documents?**

   Receipts will be required for documents transmitted by mail, to ensure that they arrived at their intended destination. Documents that are hand delivered do not require receipts.

8. **Does the new accountability procedure apply to parts?**

   Parts will be treated the same as documents for security purposes. However, if inventory and accountability procedures are required to determine stock levels, output, etc., they may be maintained as a manufacturing procedure.

9. **How do I know who the recipients of my documents are in the event a change must be distributed?**

   The address element or distribution page should list all recipients. If additional copies are distributed later, they should be penned in on the file copy. If a recipient makes copies for further distribution, they should add those to the distribution list on their copy and they will be responsible for ensuring the added recipients receive changes.

10. **Are copy and series numbers still required?**

    Copy and series numbers are no longer required for documents not in accountability.

11. **How will document control activities be inspected?**

    Inspections will be conducted according to the activities' approved procedures, security plans, and current DOE Orders and policy memoranda.

12. **Are page counts required?**

The method for counting pages and documenting the page count on the front of the document will not change.

13. **What measures need to be taken to enhance control of classified matter that is no longer in accountability?**

The most effective measure is security awareness training that emphasizes personal responsibility to adhere to the spirit and intent of DOE policy on the protection of classified matter. Penalties assessed for security infractions should be more severe than in the past because of the individual's more responsible role in the program. More stringent controls on copiers and facsimile machines must also be considered. For example, local procedures may require a supervisor's approval before copying any classified matter or copiers and facsimile machines may be relocated in areas where they are under surveillance. Increased physical controls may create inconveniences, but they will be necessary to ensure protection of classified matter.

14. **Are any jobs or work load factors affected by the changes?**

There may be some work load savings from reduced accountability procedures. However, we suspect it will be necessary to reapply savings to accommodate expanded training and physical controls requirements.

15. **Are unaccounted-for document reports still required?**

Although it is more difficult to determine when documents are lost, misfiled, or otherwise unaccounted for, the requirement to report and conduct inquiries remains in effect. This point must be emphasized during training sessions.

16. **What happens to accountability records after matter is removed from accountability systems?**

Both electronic and manual records must be retained for the retention periods required by the Records Inventory and Disposition Schedule and DOE Order 5635.1A.

17. **When will a new DOE Order be issued to formalize the new procedures?**

Page changes to the existing DOE Order 5635.1A have been staffed and should be published within 60 days. A complete rewrite of the Order, which

was previously coordinated with all activities, will be delayed until the new changes are incorporated.

18. **Are inventories still required every 36 months?**

Matter remaining in accountability must still be inventoried every 36 months, or more frequently if required by other directives or agreements, i.e., every 12 months for Top Secret, United Kingdom, and NATO matter.

ited States Government — Department of Energ

memorandum

DATE: MAY 1 6 1992

REPLY TO ATTN OF: SA-123

SUBJECT: Accountability Requirements for Secret Documents

TO: Distribution

Accountability requirements are being modified for organizations that have completed a 100 percent inventory and reconciliation in accordance with DOE Order 5635.1A, and conducted damage assessments in accordance with 32 CFR Chapter XX. Organizations fulfilling these requirements are no longer required to account for matter classified as Secret. Secret matter removed from accountability must be confined to limited areas or exclusion areas as defined in DOE Order 5632.5. Accountability of matter that is mandated by National requirements (i.e., crypto) must continue to comply with the National requirements. This action does not discourage the use of internal control systems, manual or electronic, that are used to track documents as they move within an organization.

The modified accountability requirements omit the requirements for unique document numbers, maintaining accountability records of documents, inventories, annotations of copy and series, destruction certification, written authorization to reproduce, and internal receipting. All other requirements of DOE Order 5635.1A, "Control of Classified Documents and Information" must be met. This includes, but is not limited to, page numbering, marking classification information, and requirements for transmission outside of approved buildings or facilities. Also, records of documents removed from accountability shall be retained in accordance with DOE Order 5635.1A.

Organizations that have not completed the 100 percent inventory, reconciliation, and damage assessments must continue to maintain accountability for all Secret and Top Secret matter. These organizations should continue to provide monthly inventory status reports as required by TWX dated July 20, 1989, from OP-34 to Distribution, subject: Classified Document Control 100 Percent Inventory Status Report.

For organizations meeting the criteria identified in the first paragraph, this memorandum modifies the accountability requirements contained in DOE Order 5635.1A, Chapter V. DOE Order 5635.1A is being revised to reflect this change.

Any organization requiring additional information on accountability requirements should contact Cathy Tullis on (301) 903-4805.

George T. Hersey
Director
Office of Security Affairs

Enclosure 3

United States Government

Department of Energy

memorandum

Field Office, Albuquerque
Kirtland Area Office

DATE

REPLY TO ATTN OF KAO:AB

SUBJECT Request for Implementation of Modified Accountability Requirements

TO J. D. Martin, 7400, SNL, Albuquerque

Reference is made to the Martin/Gurule October 6, 1992 memorandum, same subject.

As stated in the attached Albuquerque Field Office memorandum, Sandia National Laboratories, New Mexico, has received approval to implement the modified accountability program for Secret matter. Please ensure that all cleared personnel are aware of the new procedures and responsibilities.

If you have any questions or need additional information, please contact Stacy Kubasek at 845-5416.

Brenda J. Harmeson
Brenda J. Harmeson
Chief, Administrative Branch
Kirtland Area Office

Attachment

United States Government | Department of Ener

memorandum

Albuquerque Field Offi

DATE: OCT 3 0 1992

REPLY TO ATTN OF: SNSD:OPR:GAJ

SUBJECT: Request for Implementation of Modified Accountability Requirements

TO: K. A. Carlson, Area Manager, KAO

Reference is made to the Harmeson/Gurule October 19, 1992 memorandum, same subject.

Your request to implement the modified accountability program for Secret matter is approved, effective upon completion of the training program to advise all cleared personnel of the new procedures and their responsibilities.

Questions may be directed to Gary Jones at 845-4157.

David A. Gurule
Director, Security and
Nuclear Safeguards Division

NOV 0 2 1992

Enclosure 4

To: J. A. Kaiser, 7442

Sandia National Laboratories

Albuquerque, New Mexico 87185

February 3, 1993

All Document Accountability Station (DAS) Supervisors and Custodians

From: J. D. Martin, 7400, and J. A. Kaiser, 7442

Subject: Implementation of Modified Accountability

Sandia National Laboratories, New Mexico, has received approval to implement the modified accountability program for Secret matter. Although this policy also applies to Secret material, only Secret document controls are being addressed in this memo.

The modified accountability program omits the requirements for unique document numbers, copy and series, maintaining accountability records of documents, inventories, destruction certificates, written authorization to reproduce, and some internal receipting. A receipt must be used for all Secret information being transmitted outside of a facility or sent between facility security areas. The requirement for transmitting Secret matter outside of facilities is mandated by Federal Regulation (32 CFR).

Not only do the new requirements relieve us of accountability for Secret documents, but DOE has stated they will not fund this effort. Accordingly, the new policy precludes us from supporting PC/DAS as a Secret document accountability system. Costs associated with document accountability will be calculated only for documents for which we are held accountable.

Your current records must be kept for five years after the effective date of implementation of modified accountability. Section III of the Office Procedures Manual is being revised to include the new procedures, and copies of the updated Office Procedure Manual Section III will be distributed at the training sessions to be held on:

March 4, 1993, 10:00 a.m. - 12:00 p.m. at the TTC
March 5, 1993, 10:00 a.m. - 12:00 p.m. at the TTC
March 9, 1993, 10:00 a.m. - 12:00 p.m. at the TTC

Attendance at one session is mandatory for all Document Custodians.

These new procedures will become effective upon completion of these training programs to advise personnel of the new procedures and their responsibilities. DAS Custodians will be advised of the change-over date during the training sessions. Arrangements are being made for special classes for the new OAAs who have not received any document control training. They will be contacted directly concerning training dates.

The implementation of modified accountability is part of the National Industrial Security Program (NISP), which will standardize security requirements among all Federal agencies. Accountability of matter that is mandated by other National requirements, agreements, or special programmatic needs must continue to comply with those requirements. Some examples are: Communications Security Keying Material (Crypto), North Atlantic Treaty Organization (NATO) or Foreign Government documents, Top Secret documents, Special Access Program documents, if required by the sponsor, etc.

ML:7442-1:dr

Copy to:
0021-1 C. R. Kaemper
7141 L. Velardez
7141 A. Lucero
7142 G. Gibson
7328-3 M. Foster
7521 P. Cover
7613-2 K. Chavez
7617-2 C. Lucero
7442-1 File

Enclosure

United States Government

Department of En

memorandum

Albuquerque Field Of

DATE: MAY 17 1993

REPLY TO ATTN OF: SNSD:OPR:GAJ

SUBJECT: Request for Implementation of Modified Accountability Requirements

TO: K. A. Carlson, Area Manager, KAO

Reference is made to the May 7, 1993 Harmeson/Muller memorandum, same subject.

Your request to implement the modified accountability program for Secret matter is approved for the Sandia National Laboratories (SNL) facilities listed below. Implementation may occur upon completion of the training program to advise all cleared personnel of the new procedures and their responsibilities.

Facility	Facility Code
Tonapah Test Range	0500
Nevada Test Site	0499
Amarillo, TX	0503
Kauai, HI	0827

The SNL/NM facility located on Kirtland Air Force Base was previously approved in our October 30, 1993 Gurule/Carlson memorandum, same subject. Neither of these approvals extend to other SNL or subcontractor facilities not specifically identified by location and facility code.

Questions may be directed to Gary Jones at 845-4157.

David A. Gurule
Director, Security and
Nuclear Safeguards Division

cc:
L. J. Hofferth, SNSD, AL

Mrs. WILSON. So basically you were told by DOE Albuquerque that you could have a higher standard if you wanted to but it was going to be at no cost to the government?

Mr. ROBINSON. Correct.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. UPTON. Thank you. I just have one further question and then a comment. We are expecting a vote in the next 5 or 10 minutes. Mr. Glauthier, I know you have a meeting downtown as well, and I will let other members ask if they have additional questions.

Dr. Browne, the list of new controls that you mentioned in your testimony, you did not include procedures to ensure that those who remove materials from vaults check out such documents or disks. And I just wondered why you did not include that type of reform. And I am wondering, maybe from General Habiger, in terms of why that was not required in his June 23 list of new security directives. Dr. Browne?

Mr. BROWNE. With respect to the NEST program, we have had that vault closed as part of the FBI investigation and have done a full inventory of all the NEST equipment.

So that program is sort of an off-limits program right now.

With respect to all the other information, until we reestablish tracking ability for the documents, we don't have a mechanism to find where the information goes. We have started down that path with the computer storage media that I mentioned earlier, the 66,000 devices. So we can track those, but we are not in a position to track everything that comes out of a vault unless it is done by hand; you know, the name of the person, et cetera. We have not done that.

Mr. UPTON. Do you expect to have some type of tracking, whether it be a bar code or something of that nature?

Mr. BROWNE. That's what we had before, and the mechanism for transfer of documents between one individual and another one required a tracking of the bar code and the copy number, and so one had a record of when it left and went somewhere else.

Mr. UPTON. And are you on the path to encrypt some of this data as well?

Mr. BROWNE. That's correct. That's part of the Department's——

Mr. UPTON. On both Top Secret and Secret data material?

Mr. BROWNE. That's correct.

Mr. HABIGER. Mr. Chairman, the big problem we have with encryption is that we have one certified software package that is only good for Windows NT. The Department of Energy had many, many operating systems. The vendor tells us it could be up to a year before we are able to have other operating systems covered.

Mr. UPTON. General McBroom, what has happened to this particular NEST team while the investigation is going on? Are they in limbo? Have they gone back to their other functions?

Mr. MCBROOM. Well, sir, that's really a lab question. I haven't been allowed out there or to see them. I am going out there next week. I can tell you in talking to Dr. Browne, they have been through a lot, sir. Personally and professionally it has been very hard on them.

We are going to have to really stroke some of these people because—and I think Dr. Browne had a very, very valid point. Nine-

ty-nine percent of these people are just really neat United States American citizens.

Mr. UPTON. You need to find that 1 percent.

Mr. MCBROOM. Yes, sir, I have to find them in a hurry.

Mr. GIOCONDA. Sir, also for the record to understand, the NEST team are a group of volunteers. They volunteer to be in this program. They are not assigned to this particular program. They step up to be assigned. I think that it is important to understand that when you go through a situation like this, and we have talked about this often, what are we going to have on Monday morning. Will that person volunteer after going through this? And we are all very, very concerned about that.

Mr. BROWNE. Mr. Chairman, may I add a comment to that?

Mr. UPTON. Yes.

Mr. BROWNE. What we did with our NEST team was essentially had the entire team stand down to go through in great detail their security procedures for the entire team, not just the device assessment team that I mentioned but the entire team, because we wanted them to update all of their security procedures and to assure themselves, not just assure us but assure themselves that they had the best practices in place. They have just completed that and they are back at work.

We have some compensatory measures in place because of the FBI investigation that's going on, but I feel very comfortable that we are doing the right thing by allowing the NEST team members back to work.

Mr. UPTON. Mr. Glauthier, I know you mentioned at the very beginning of your testimony sort of the update in terms of where we were with regard to the investigation. I am certainly not a police officer or a detective, as my colleague Mr. Stupak was with the Michigan State Police. But are we getting close to the end of this? I mean, I know that a number of folks, in fact, were polygraphed. It has been almost a month since those began. Where are we in terms of the end of this investigation so we can put things back together?

Mr. GLAUTHIER. I think it is all right to mention here that one of the delays has been that the lawyers for these individuals felt they needed to get clearances in order to properly deal with their clients and to deal with these issues. Those clearances were granted last week. It took some time for them to submit the paperwork to us. We turned it around in a matter of few days.

Mr. UPTON. But they were polygraphed almost from the beginning, right? June 15 or so?

Mr. GLAUTHIER. The individuals were, but the lawyers representing those individuals needed to get clearances, they said, in order to proceed with the case. So some of the investigation has been on hold. Now, those clearances have been in place for a matter of a few days at least and I understand that the FBI and the U.S. Attorney out there are proceeding.

Our hope is that this will——

Mr. UPTON. Do you expect some charges to be brought within this month, July?

Mr. GLAUTHIER. You would have to ask the FBI and the U.S. Attorney's Office. I can't comment on that.

Mr. UPTON. Okay. Let me just say this, as part of my conclusion. As Chairman of this subcommittee, we have had more hearings on security at our energy labs than on any other topic—Medicare fraud, anything else—maybe, I would guess, 12 to 15 hearings in the last year and a half.

At the suggestion of the lab directors last year, for a number of us that had not ever been to one of these labs and really not been to the West Coast much, I know that we did take your suggestion. We visited the labs, and I have to say that for me, I could not have been more impressed with the physical security of those labs; the drills that the teams did, all the different things that were shown to us over those couple of days, Mr. Cox, myself, Mr. Burr and Mrs. Wilson and some of our staff that went out.

It seems as though we have focused on—we have gone from one thing to the next.The hearings last year followed along the lines of the Q clearances and the access to some of our secret material by folks that really should not have been in those areas. Changes were made.

One of the things that we focused quite a bit on in our visit last January was looking at the cyber security details and to make sure that there were air locks and a whole number of different things that would prevent someone from hacking in and getting access to that material.

I just hope that as we have looked now at this GAO report, that again it sort of goes back to the basics, logging in material; I mean, what we can do at a Meyers, a Thrifty Acres, or maybe a Safeway here in the Washington area type of thing, a library logging in material using the tools that we have, encryption and others, to make sure that, in fact, that material—you know, if we find that 1 percent that, in fact, may be out there that, in fact we can prevent that individual or individuals from leaking or selling that information someplace else, let alone misplacing it, I mean that to me is fundamental.

We—as Chairman of this subcommittee, and I know I speak for every member of this subcommittee—we have got to have accountability by all of you to make sure that the system works. We are tired of the blame game. We would rather be focusing on other things than this. But these really are the crown jewels. And whether it is a culture, whether it is just mistake after mistake, we need to get to the bottom of this and we need to get it resolved. We don't necessarily need another level of bureaucracy. We want results and we want to know that when the lights get turned off, that that material is safe and cannot get into the hands of the wrong people.

Virtually every one of you, with the exception of Mr. Aftergood, are Federal employees; particularly General McBroom and others, you need to take every effort. We are prepared as a Congress to fund whatever it takes to make sure that these secrets remain just that. Now you have a tremendous responsibility. The American public has entrusted you and we want to make sure it works. I would just hope that as we follow up on this hearing today that, in fact, we won't see further miscues.

Mr. Glauthier, your comment earlier about taking the pledge—I think it was by Mr. Bilbray—by January 1, Secretary Richardson did that. You might have offered him some different advice last

year when he assured us in fact that those things would not take place. We want your word to be good and we want the fire doors to be closed so that this does not happen again.

As we look at further GAO reports and other things that may come our way, we want to hear from you first and see what suggestions you might have that we might help you do a better job to make sure that, in fact, that fire door remains closed.

Mr. Cox, I don't know if you want to make a closing statement, Mrs. Wilson, but I yield to you if you would like to do that.

Mr. COX. I thank you, and I just want to thank every member of our panel. These are difficult topics and they are made more difficult by the fact that there have been so many things that everybody wishes hadn't happened go on over the last few years.

My greatest concern is the seeming consistency of the bureaucratic problems, notwithstanding all of the renewed vigor to attack them at this time and to get it right.

When the House of Representatives nearly unanimously created this select committee that I chaired, it was 4 months after the President had issued PDD 61, and then we went through a whole year on our select committee and had more public impact with that, and then we had damage assessment by the CIA which confirmed what our select committee had found. We had the President's Foreign Intelligence Advisory Board complain about security and counterintelligence at the laboratories and about DOE mismanagement. We had recommendations for reform. And yet it was not until March of this year that one of the key elements of the President's directive to the Secretary of Energy, polygraphing, was even begun to be implemented.

It was not really until these hard drives turned up missing that people in sensitive positions in that connection were subjected to polygraphs. I think that it is a fair thing to argue, particularly for scientists who are technically minded, to argue about the relative merits and demerits of polygraphs. They are well equipped to do so. But once the President of the United States orders it done, it oughtn't take the bureaucracy so many years to begin it.

The same holds with the creation of the NNSA. The NNSA was created in direct response to recommendations from all the outside groups that have looked at it and the bureaucracy has been fighting it because of turf. Now we are talking about new creative ways to restructure the bureaucracy, all of them compounding the prolix nature of the Department of Energy's relationship to the labs, and I am very sorry for that. I hope that one of these days they will listen to the advice and follow the legislation.

I thank the chairman.

Mr. UPTON. Thank you. Mrs. Wilson, do you have a closing comment?

Mrs. WILSON. Thank you, Mr. Chairman. I wanted to thank you again for allowing me to sit in and participate in this hearing. I think I walk away with kind of a reconfirmation that the problems relating to security in the nuclear weapons complex are systemic. They relate more to policy and the implementation of that policy than they do to isolated acts by individuals. And I look forward to General Gordon taking the reigns and being able to look at the complex systematically over a long period of time to ensure its con-

tinued health for the country, and I think that's the right direction to go in. And I thank the chairman again.

Mr. UPTON. Again, I thank all members for participating. I would note for the record that there are a number of subcommittees meeting during these hours. We do look forward to hearing from General Gordon probably this fall, once Congress returns from the August break. Again we thank you for your testimony. We look forward to working with you. This hearing is now adjourned.

[Whereupon, at 2:55 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

FEDERATION OF AMERICAN SCIENTISTS
August 1, 2000

Hon. FRED UPTON, *Chairman*
Subcommittee on Oversight and Investigations
Committee on Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

DEAR MR. CHAIRMAN: Attached please find my answers to the questions for the record from the July 11, 2000 hearing on weaknesses in classified information security control's at DOE's nuclear weapons laboratories.

Thank you for the opportunity to present my views to the Subcommittee.

Sincerely,

STEVEN AFTERGOOD
Senior Research Analyst

QUESTIONS FOR STEVEN AFTERGOOD

Q. In your testimony, you quoted a National Academy of Sciences report which states that "access to classified information is not necessary for a potential proliferator to construct a nuclear weapon." The Academy said that access to nuclear material and an engineering and manufacturing infrastructure to build a bomb are most important. Iraq became a nuclear power without stealing our secrets, as did India. Was the Cox Commission and the Congress in error last year when they placed so much emphasis on the alleged theft of our technology for China's weapons advances?

A. The espionage threat from China and other nations is certainly a legitimate and necessary subject of inquiry. But I believe the Cox Committee and Congress erred by failing to place the espionage threat in proper perspective.

The People's Republic of China has possessed thermonuclear weapons since 1964 and has a mature nuclear weapons manufacturing capacity. Yet today, *fifteen years* after China's alleged theft of W-88 warhead design information described by the Cox Committee, there has been no "apparent modernization of their deployed strategic force or any new nuclear weapons development," according to the CIA's Jeremiah panel. Espionage, if it occurred, evidently did little to alter the threat facing the United States.

Instead of clarifying the issues, the continuing emphasis on Chinese nuclear espionage has led to a serious distortion of public perceptions. Senator Bob Kerrey said last year that the Cox Committee report "has left the impression that China is a bigger threat to the United States in terms of nuclear weapons than Russia is. Nothing can be further from the truth." But a Time-CNN public opinion poll found that 46 percent of Americans consider China a serious threat, compared to 24 percent who hold that view of Russia.

Finally, the preoccupation with espionage has incurred serious damage to the nuclear weapons laboratories where morale a,'Id recruitment have fallen precipitously. This is a potentially far more serious blow to national security than any espionage that may have taken place.

Q. What do you see as the solution to these embarrassing security breaches at DOE?

A. There is no solution. That is to say, it is impossible to guarantee that security breaches will not occur in the future.

Again, it is important to keep these matters in perspective. There can be no absolute security. There is no national security agency in the U.S. government that has not been deeply penetrated by a foreign intelligence service at one time or another. Meanwhile, minor security infractions are literally a daily occurrence.

It is easier to say what is *not* the solution. I do not believe that Congress should legislate specific security requirements (such as document accountability, polygraph screening, etc.) because such system-wide requirements can have unintended consequences and may need to be modified to meet local needs and circumstances.

On the other hand, it would be appropriate to identify an official at each facility who is responsible for security at that facility. While I believe it was absurd to suggest that the Secretary of Energy should be accountable for the fact that a particular classified item at Los Alamos was missing, it would be entirely sensible to assign responsibility for such cases to a particular official at every laboratory. That official should have the flexibility and discretion to tighten or relax baseline security requirements, as appropriate, and then should be held responsible for overall security performance.

I would only add, as I stated in my testimony, that security should not be permitted to significantly erode the quality of the labs. If it were necessary to choose, I would prefer second-rate security at a first-rate laboratory to first-rate security at a second-rate laboratory.

Q. What will it take to implement the "higher fences" initiative?

A. The "higher fences" concept of focusing security resources on the most sensitive information makes obvious, intuitive sense. But like any change to established practices in a bureaucracy, it faces resistance that will require high-level leadership to overcome.

DOE officials now refer to the adoption of a "graded approach" to security, involving stronger protection for more sensitive materials, The "graded approach" seems to be similar to the "higher fences" initiative except that it *omits declassification.*

This is a mistake, in my opinion. Proper declassification is an essential component of an information security classification system. The system will not function properly, and will eventually break down, if there is no reliable mechanism for removing controls on information that no longer warrants protection.

For this reason, I believe that the DOE Fundamental Classification Policy Review group (which last reported in 1997) should be reconvened at perhaps 5-year intervals to identify which categories of information should be newly declassified and which categories, if any, should receive increased protection.

I also believe that Congress should increase support for declassification review. Congress should clearly communicate to DOE the expectation that while sensitive information must be properly classified, information that is no longer sensitive should be efficiently removed from classification controls.

ANSWERS TO QUESTIONS FOR THE RECORD OF DR. C. PAUL ROBINSON, DIRECTOR, SANDIA NATIONAL LABORATORIES

Question: The Committee understands that Sandia played a big role in the Higher Fences initiative. Can you describe your lab's involvement and why you believe DOE has not reached closure on this issue after four years of trying?

Did Sandia object to DOE's initial proposal on higher fences, and if so, why?

Did Sandia object to reclassifying these sensitive categories as Top Secret, and if so, why? What value would there be in re-classifying these sensitive topics as Top Secret, as proposed by DOE, if DOE didn't require additional controls for Top Secret, as evidenced by its January 1998 decision to eliminate such controls?

Response: Sandia National Laboratories was a major participant and contributor in the Higher Fences Initiative beginning with the Fundamental Classification Policy Review, which began its work in May 1995. Secretary O'Leary appointed Dr. Albert Narath, the director of Sandia, to be chairman of the review group. (It should be noted that Dr. Narath left Sandia in August 1995 to accept a position with the Lockheed Martin Corporation. He continued to chair the review team while in his new position.) The Fundamental Classification Policy Review Group consisted of about 50 experts from the DOE community and other agencies, including several individuals from Sandia. The review team issued a final report in January 1997.

Sandia National Laboratories also played a major role on the second of two Higher Fences working groups. A first working group had been formed at DOE headquarters shortly after the Fundamental Classification Policy Review issued its report, but the results of this first effort were deemed inadequate by many reviewers in the field and at headquarters. The considerable criticism of the first working group's proposal prompted the DOE Office of Declassification to charter a second Higher Fences Working Group in July 1998 to resolve the issues identified in the critiques. The DOE Office of Declassification appointed the classification officer at Sandia National Laboratories to lead this group of classification experts from the field and DOE.

Sandia National Laboratories fully supported (and continues to support) the initial Higher Fences recommendation of the Fundamental Classification Policy Review Group (January 1997). However, Sandia and other DOE elements in the field and at headquarters had several criticisms of the work of the first Higher Fences Working Group, which issued a memorandum for comment in March 1998. That report received a largely negative response. A major concern shared by Sandia and the other nuclear weapon laboratories was that DOE had recently removed (in January 1998) the longstanding requirement for formal document accountability of Top Secret Restricted Data. To classification professionals in the field, it seemed inconsistent to propose to reclassify certain information to Top Secret while at the same time weakening the accountability controls on Top Secret. Thus, reclassification on the Higher Fences criteria would be a paper exercise resulting in no significant increase in protection within the DOE community.

In May 1998, the DOE Technical Evaluation Panel submitted its concerns on the initial Higher Fences guidance in a memorandum to the director of the DOE Office of Security Affairs. The Technical Evaluation Panel is a committee of weapon designers that provides consultation for the DOE classification community, and it was chaired at that time by a Sandia weapon program manager. The panel's basic criticism of the initial Higher Fences guidance was that the lack of consistency in the level of protection provided for Top Secret Restricted Data by the various DOE orders governing security of documents and computer systems undermined the initiative. The panel predicted that these inconsistencies, together with the failure to address the costs of implementation, would result in failure of the Higher Fences Initiative.

The second Higher Fences Working Group issued an unclassified draft report to the DOE Office of Declassification in February 1999, followed by a full, classified report in April. The report filled in some of the detail that would be required for implementation and added much-needed rigor to the sensitivity criteria for reclassification. This work provided a foundation for moving forward with the Higher Fences Initiative within the Department's decision structure, and eventually to DoD.

DOE issued a final report for implementing the Higher Fences recommendation in October 1999. At that point, considerable disagreement still existed both within the Department and in the field concerning how Higher Fences should be implemented, although the concept and intent of the Higher Fences Initiative were generally accepted. The most significant issues of concern were:

1. DOE's decision in January 1998 to remove the requirement for formal document accountability for Top Secret Restricted Data;
2. The lack of consistent guidance within DOE on handling paper and electronic forms of Top Secret;
3. The lack of implementation guidance and associated funding for segregating new Top Secret and handling existing Top Secret;
4. The lack of funding to upgrade Secret-level computer networks to Top Secret networks, which was estimated to run $20 to $30 million per site.

Notwithstanding these concerns, the DOE leadership decided to press forward with implementation. In October 1999, the Assistant Secretary for Defense Programs and the Director of the Office of Security and Emergency Operations sent a letter to the Nuclear Weapons Council (a joint DoD/DOE coordinating group of senior officials) requesting the assistance of the Council in encouraging DoD to participate in a joint working group to develop an implementation plan for Higher Fences. Buy-in by DoD was essential because much Secret Restricted Data that would be reclassified to Top Secret under the Higher Fences plan was in the custody of DoD.

In December 1999, DOE received a response from the Office of the Secretary of Defense (signed by the director of Defense Research and Engineering and by the Assistant Secretary for Command, Control, Communications, and Intelligence) in which DoD declined to participate in an interagency working group for the Higher Fences Initiative. The letter cited increased costs, operational difficulties, and DoD's belief that such information is adequately protected at the Secret level. The letter also indicated that DoD would review the Higher Fences recommendations from a cost-benefit perspective so that the initiative could receive serious consideration. At this time, I am unaware that DoD has completed its review. However, the evident lack of serious interest by DoD is the principal reason for the failure of the Higher Fences Initiative to continue to move forward toward implementation.

GENERAL ACCOUNTING OFFICE RESPONSES TO QUESTIONS FOR THE RECORD

Q. Was the 1992 change in DOE Secret-level accountability controls mandated by Executive Order or government-wide changes that occurred in that year, as DOE has suggested in article in the *Washington Post*, or was DOE free to set its own policies in this regard?

A. The 1992 change in DOE Secret-level accountability controls was not mandated by Executive Order or any government-wide requirements as far as we can determine. The Executive Order in force at the time—EO 12356, dated April 2, 1982, and its implementing directive-allowed heads of agencies to set policies for accountability for Secret-level documents. Therefore, DOE could set its own policies within this framework.

Q. This same article also states that, in January 1993, just two weeks before the end of the Bush Administration, an executive order extended these new relaxed rules to government contractors, such as Los Alamos. Is that an inaccurate statement based on your research? What did the Executive Order actually do? Please provide a copy of the Executive Order for the record.

A. The statement "in January 1993, just two weeks before the end of the Bush Administration, an executive order extended these new relaxed rules to government contractors, such as Los Alamos" is inaccurate. Executive Order 12829, dated January 6, 1993, created a National Industrial Security Program to establish a single, integrated, cohesive program to protect classified information that is released to contractors, licensees, and grantees of the United States Government. While the Program was created to promote uniformity, the Executive Order did not specify that accountability requirements were to be relaxed.

Q. To your knowledge, was there any government-wide decision made to reduce controls on Secret data prior to 1995?

A. Our audit work concentrated on DOE actions in accountability for Secret documents. As such we did not examine what other government agencies were doing to control Secret data. We will examine this issue as part of our ongoing work in the area.

in a manner that does not deviate from the "set of ideas."

The Secretary General, in paragraph 59 of his report, indicated that intensive efforts had failed to produce an overall agreement, and he concluded that the lack of political will mentioned in his previous report "continues to block the conclusion of an agreement that is otherwise within reach." He noted in the following paragraph that the Security Council had asked in its Resolution 774 (provided with my last letter) that, should an agreement not be reached, the Secretary General should recommend alternative courses of action to resolve the Cyprus problem. Subsequent paragraphs outline his proposals, including a number of measures to help create a new climate of confidence between the two parties, which would contribute to the success of the negotiating process. These confidence-building measures are outlined in paragraph 63 of the Secretary General's report.

On November 25, the U.N. Security Council adopted its Resolution 789, which endorsed the U.N. Secretary General's report of November 19, and urged both sides to commit themselves to the Secretary General's series of confidence-building measures, including initiating a significant reduction of foreign troops and defense spending on the island.

I am happy to note that, before departing New York in November, the parties agreed to resume their face-to-face negotiations in March 1993, which will be after the presidential elections in the Republic of Cyprus scheduled for February 7, 1993. We would have preferred, of course, that the October-November round of negotiations would have proceeded beyond the point of defining positions and differences and would have entered the phase of bridging gaps between the positions of the parties and the U.N. "set of ideas," including the Secretary General's map, which remains the basis for negotiations for a fair and permanent resolution that would benefit all Cypriots.

I continue to believe and to agree with the statement in Security Council Resolution 789 that the present status quo is not acceptable. An overall agreement in line with the U.N. "set of ideas" should be achieved without further delay. I also urge all concerned to commit themselves to the implementation of the confidence-building measures set out in Resolution 789 and to come to the next round of talks prepared to make the difficult decisions that will bring about a speedy agreement.

Sincerely,

George Bush

Note: Identical letters were sent to Thomas S. Foley, Speaker of the House of Representatives, and Claiborne Pell, Chairman of the Senate Committee on Foreign Relations.

Executive Order 12829—National Industrial Security Program

January 6, 1993

This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.

Therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, including the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011–2286), the National Security Act of 1947, as amended (codified as amended in scattered sections of the United States Code), and the Federal Advisory Committee

Act, as amended (5 U.S.C. App. 2), it is hereby ordered as follows:

PART 1. ESTABLISHMENT AND POLICY

Section 101. *Establishment.* (a) There is established a National Industrial Security Program. The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. For the purposes of this order, the terms "contractor, licensee, or grantee" means current, prospective, or former contractors, licensees, or grantees of United States agencies. The National Industrial Security Program shall be applicable to all executive branch departments and agencies.

(b) The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order No. 12356 of April 2, 1982, or its successor, and the Atomic Energy Act of 1954, as amended.

(c) For the purposes of this order, the term "contractor" does not include individuals engaged under personal services contracts.

Sec. 102. *Policy Direction.* (a) The National Security Council shall provide overall policy direction for the National Industrial Security Program.

(b) The Director of the Information Security Oversight Office, established under Executive Order No. 12356 of April 2, 1982, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:

(1) develop, in consultation with the agencies, and promulgate subject to the approval of the National Security Council, directives for the implementation of this order, which shall be binding on the agencies;

(2) oversee agency, contractor, licensee, and grantee actions to ensure compliance with this order and implementing directives;

(3) review all agency implementing regulations, internal rules, or guidelines. The Director shall require any regulation, rule, or guideline to be changed if it is not consistent with this order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation, rule, or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority, pursuant to terms of applicable contracts, licenses, grants, or regulations, to conduct on-site reviews of the implementation of the National Industrial Security Program by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific classified information, or other forms of cooperation, would pose an exceptional national security risk, the affected agency head or the senior official designated under section 203(a) of this order may request the National Security Council to deny access to the Director. The Director shall not have access pending a prompt decision by the National Security Council;

(5) report any violations of this order or its implementing directives to the head of the agency or to the senior official designated under section 203(a) of this order so that corrective action, if appropriate, may be taken. Any such report pertaining to the implementation of the National Industrial Security Program by a contractor, licensee, or grantee shall be directed to the agency that is exercising operational oversight over the contractor, licensee, or grantee under section 202 of this order;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the National Industrial Security Program;

(7) consider, in consultation with the advisory committee established by this order, affected agencies, contractors, licensees, and grantees, and recommend to the President through the National Security Council changes to this order; and

(8) report at least annually to the President through the National Security Council on the implementation of the National Industrial Security Program.

(c) Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Com-

mission under the Atomic Energy Act of 1954, as amended, or the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order No. 12333 of December 8, 1981.

Sec. 103. *National Industrial Security Program Policy Advisory Committee.* (a) *Establishment.* There is established the National Industrial Security Program Policy Advisory Committee ("Committee"). The Director of the Information Security Oversight Office shall serve as Chairman of the Committee and appoint the members of the Committee. The members of the Committee shall be the representatives of those departments and agencies most affected by the National Industrial Security Program and nongovernment representatives of contractors, licensees, or grantees involved with classified contracts, licenses, or grants, as determined by the Chairman.

(b) *Functions.* (1) The Committee members shall advise the Chairman of the Committee on all matters concerning the policies of the National Industrial Security Program, including recommended changes to those policies as reflected in this order, its implementing directives, or the operating manual established under this order, and serve as a forum to discuss policy issues in dispute.

(2) The Committee shall meet at the request of the Chairman, but at least twice during the calendar year.

(c) *Administration.* (1) Members of the Committee shall serve without compensation for their work on the Committee. However, nongovernment members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(2) To the extent permitted by law and subject to the availability of funds, the Administrator of General Services shall provide the Committee with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(d) *General.* Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

PART 2. OPERATIONS

Sec. 201. *National Industrial Security Program Operating Manual.* (a) The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence, shall issue and maintain a National Industrial Security Program Operating Manual ("Manual"). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended. The Director of Central Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information.

(b) The Manual shall prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information to contractors, licensees, or grantees. The Manual shall apply to the release of classified information during all phases of the contracting process including bidding, negotiation, award, performance, and termination of contracts, the licensing process, or the grant process, with or under the control of departments or agencies.

(c) The Manual shall also prescribe requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information.

(d) In establishing particular requirements, restrictions, and other safeguards within the Manual, the Secretary of Defense, the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence shall take into account

these factors: (i) the damage to the national security that reasonably could be expected to result from an unauthorized disclosure; (ii) the existing or anticipated threat to the disclosure of information; and (iii) the short- and long-term costs of the requirements, restrictions, and other safeguards.

(e) To the extent that is practicable and reasonable, the requirements, restrictions, and safeguards that the Manual establishes for the protection of classified information by contractors, licensees, and grantees shall be consistent with the requirements, restrictions, and safeguards that directives implementing Executive Order No. 12356 of April 2, 1982, or the Atomic Energy Act of 1954, as amended, establish for the protection of classified information by agencies. Upon request by the Chairman of the Committee, the Secretary of Defense shall provide an explanation and justification for any requirement, restriction, or safeguard that results in a standard for the protection of classified information by contractors, licensees, and grantees that differs from the standard that applies to agencies.

(f) The Manual shall be issued no later than 1 year from the issuance of this order.

Sec. 202. *Operational Oversight.* (a) The Secretary of Defense shall serve as Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees. The heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

(b) The Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf.

(c) The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended. The Secretary or the Commission may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on behalf of the Secretary or the Commission, respectively.

(d) The Executive Agent shall have the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the National Industrial Security Program.

Sec. 203. *Implementation.* (a) The head of each agency that enters into classified contracts, licenses, or grants shall designate a senior agency official to direct and administer the agency's implementation and compliance with the National Industrial Security Program.

(b) Agency implementing regulations, internal rules, or guidelines shall be consistent with this order, its implementing directives, and the Manual. Agencies shall issue these regulations, rules, or guidelines no later than 180 days from the issuance of the Manual. They may incorporate all or portions of the Manual by reference.

(c) Each agency head or the senior official designated under paragraph (a) above shall take appropriate and prompt corrective action whenever a violation of this order, its implementing directives, or the Manual occurs.

(d) The senior agency official designated under paragraph (a) above shall account each year for the costs within the agency associated with the implementation of the National Industrial Security Program. These costs shall be reported to the Director of the Information Security Oversight Office, who shall include them in the reports to the President prescribed by this order.

(e) The Secretary of Defense, with the concurrence of the Administrator of General Services, the Administrator of the National

Aeronautics and Space Administration, and such other agency heads or officials who may be responsible, shall amend the Federal Acquisition Regulation to be consistent with the implementation of the National Industrial Security Program.

(f) All contracts, licenses, or grants that involve access to classified information and that are advertised or proposed following the issuance of agency regulations, rules, or guidelines described in paragraph (b) above shall comply with the National Industrial Security Program. To the extent that is feasible, economical, and permitted by law, agencies shall amend, modify, or convert preexisting contracts, licenses, or grants, or previously advertised or proposed contracts, licenses, or grants, that involve access to classified information for operation under the National Industrial Security Program. Any direct inspection or monitoring of contractors, licensees, or grantees specified by this order shall be carried out pursuant to the terms of a contract, license, grant, or regulation.

(g) Executive Order No. 10865 of February 20, 1960, as amended by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, is hereby amended as follows:

(1) Section 1(a) and (b) are revoked as of the effective date of this order.

(2) Section 1(c) is renumbered as Section 1 and is amended to read as follows:

"***Section 1.*** When used in this order, the term 'head of a department' means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term 'head of a department' also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829."

(3) Section 2 is amended by inserting the words "pursuant to Executive Order No. 12829" after the word "information."

(4) Section 3 is amended by inserting the words "pursuant to Executive Order No. 12829" between the words "revoked" and "by" in the second clause of that section.

(5) Section 6 is amended by striking out the words "The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section (1)(b)," at the beginning of the first sentence, and inserting in their place "The head of a department of the United States . . . ."

(6) Section 8 is amended by striking out paragraphs (1) through (7) and inserting in their place ". . . the deputy of that department, or the principal assistant to the head of that department, as the case may be."

(h) All delegations, rules, regulations, orders, directives, agreements, contracts, licenses, and grants issued under preexisting authorities, including section 1(a) and (b) of Executive Order No. 10865 of February 20, 1960, as amended, by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, shall remain in full force and effect until amended, modified, or terminated pursuant to authority of this order.

(i) This order shall be effective immediately.

George Bush

The White House,
January 6, 1993.

[*Filed with the Office of the Federal Register, 10:52 a.m., January 7, 1993*]

Note: *This Executive order was released by the Office of the Press Secretary on January 7, and it was published in the Federal Register on January 8.*